Part 1 SysPatron System Patron

Table of Contents i
Chapter 1 System Description 1-1
1.1 Overview of System SysPatron 1-1
1.2 Comparing with Ordinary Anti-Virus Software 1-1
1.2.1 Features of Ordinary Anti-Virus Software 1-1
1.2.2 Features of SysPatron 1-1
1.2.3 Comparison Results 1-1
1.3 Function Description 1-2
1.3.1 Overview of SysPatron Functions 1-2
1.3.2 System Verification 1-3
1.3.3 Progress Monitoring 1-4
1.3.4 Integrity Detection 1-5
1.3.5 Log Management 1-5
1.3.6 Alarm Management 1-6
1.4 Software and Hardware Configuration 1-6
1.4.1 Hardware Configuration 1-6
1.4.2 Software Configuration 1-7
Chapter 2 Installing System SysPatron 2-1
2.1 Precautions 2-1
2.2 Software Installation 2-2
2.2.1 Installation Flow 2-2
2.2.2 Preparations Before Installation 2-2
2.2.3 Installation Process 2-3
2.2.4 Installation Check 2-6
2.3 Uninstalling Software 2-8
Chapter 3 Basic Operations 3-1
3.1 Overview of Basic Operations 3-1
3.2 Generating Verification Files 3-1
3.2.1 Selecting Source Files 3-1
3.2.2 Generating Verification Files 3-2
3.3 Starting SysPatron 3-2
3.4 Stopping the SysPatron Processes 3-3
3.5 Checking the System Integrity 3-4
3.6 Checking and Processing the Alarm 3-5
3.7 Checking Log File 3-7
Chapter 4 FAQs 4-1
4.1 Overview of FAQs 4-1
4.2 Installation Terminated at License Agreement 4-1
4.3 SysPatron Cannot be Started 4-1

4.4 How to Change the Startup Type of _UM_PPT_Service_ 4-1
4.5 Need Verification Files for Commonly Used Programs? 4-2
4.6 Edit Registry Items of SysPatron? 4-2
4.7 Cannot Access Files or Use Applications After Installing SysPatron 4-2
4.8 SysPatron Still Functions After Uninstallation 4-2
4.9 SysPatron Cannot Be Reinstalled After Uninstallation 4-3
Appendix A Description of Installation Folders A-1
Appendix B Description of Configuration File B-1
B.1 Editing Description of Configuration File B-1
B.2 Description of Parameter Segments B-2
B.2.1 Overview of Parameter Segments B-2
B.2.2 Core File List [PROCESSES] B-2
B.2.3 Detection File List [FILES] B-6
B.2.4 Timing Detection Parameter [BASIC] B-7
B.2.5 Log Management Parameter [BASIC] B-9
B.2.6 Alarm Parameter [WARNING] B-11

Part 2 iWeb Remote Maintenance Access System

Table of Contents i
Chapter 1 System Description 1-1
1.1 Overview of iWeb Maintenance Access System 1-1
1.2 Service Models 1-1
1.2.1 Overview of Service Models 1-1
1.2.2 Typical Configurations 1-1
1.2.3 Configuration Guidelines 1-5
1.2.4 Remote Access Server RAS 1-7
1.2.5 Remote Access Client RAC 1-8
1.3 System Functions of iWeb system 1-10
1.3.1 Access Control of iWeb system:access control 1-10
1.3.2 Connection Management of iWeb system:connection management 1-10
1.3.3 Two-Way Data Transmission of iWeb system:two-way data transmission 1-10
1.3.4 Data Compression and Encryption of iWeb system:data compression and encryption 1-11
1.3.5 Traversing Firewalls and Proxy Servers of iWeb system:traversing firewalls and proxy servers 1-11
1.4 Technical Features of iWeb system 1-11
1.4.1 Little System Structure Change 1-11
1.4.2 Configurable Access Control Strategy 1-12
1.4.3 Compression and Encryption Based on Ports 1-12

1.4.4 Adjusted Network Bandwidth 1-12
1.4.5 Automatic Retry Connection 1-12
1.4.6 Support from Multiple Maintenance Terminals 1-12
1.5 Software and Hardware Configuration 1-12
1.5.1 Hardware Configuration 1-12
1.5.2 Software Configuration 1-13
Chapter 2 Software Installing and Uninstalling 2-1
2.1 Software Installation 2-1
2.1.1 Installation Flow 2-1
2.1.2 Installation Preparations 2-2
2.1.3 Installing JDK Software 2-3
2.1.4 Installing RAS Software 2-8
2.1.5 Check for RAS Software Installation 2-14
2.1.6 Installing RAC Software 2-16
2.1.7 Check for RAC Software Installation 2-16
2.2 Uninstalling Software 2-17
2.3 Frequently Asked Question in Software Uninstallation 2-20
Chapter 3 Operation Guide 3-1
3.1 Overview of Operation Guide 3-1
3.2 Introduction to Service Interfaces 3-1
3.2.1 RAS Service Interface 3-1
3.2.2 RAC Service Interface 3-3
3.3 RAS Data Configuration 3-4
3.3.1 Configuring IP Address and Ports. 3-5
3.3.2 Configuring Multi-Language Attribute 3-6
3.3.3 Configuring Log Functions 3-8
3.3.4 Configuring Connection Instances 3-9
3.3.5 Configuring Server Types 3-16
3.3.6 Configuring Server Instances 3-20
3.4 RAC Data Configuration 3-24
3.4.1 Configuring the System Attribute File 3-24
3.4.2 Configuring Log Functions 3-25
3.4.3 Configuring Proxy Information 3-25
3.4.4 Configuring Maintenance Terminal Access Strategy 3-27
3.5 RAS Basic Operation 3-30
3.5.1 Starting RAS Background Service 3-30
3.5.2 Logging in RAS Service Interface 3-31
3.5.3 Reviewing Connection Requests Manually 3-31
3.5.4 Changing RAS Login Password 3-33
3.5.5 Logging Out RAS 3-35
3.5.6 Showing Online Help 3-36

3.5.7 Closing RAS Background Service 3-38
3.6 RAC Basic Operation 3-38
3.6.1 Logging in RAC Service Interface 3-38
3.6.2 Changing RAC Login Password 3-38
3.6.3 Locking and Unlocking 3-39
3.6.4 Establishing/ Deleting a Connection to RAS 3-39
3.6.5 Activating/Deactivating a Connection to RAS 3-45
3.6.6 Manual-Refresh/Auto-Refresh Connection Status 3-46
3.6.7 Changing RAC Interface Display Mode 3-47
3.6.8 Showing Online Help 3-48
3.6.9 Showing the iWeb System Version Information 3-48
3.6.10 Logging Out RAC 3-49
3.6.11 Exiting RAC Service Interface 3-49
3.7 A Typical Maintenance Example 3-50
3.7.1 Description of Example 3-50
3.7.2 Configuring RAS Data 3-50
3.7.3 Configuring the RAC Data 3-50
3.7.4 Creating Connection from RAC to RAS 3-51
3.7.5 Starting Remote Maintenance 3-51
3.7.6 Ending Remote Maintenance 3-51
3.8 FAQ on Remote Maintenance 3-51
3.8.1 One RAC Cannot Activate Multiple Maintenance Terminals? 3-51
3.8.2 RAC Cannot Refresh Connection Status or Start Connection? 3-52
3.8.3 Maintenance Terminal Cannot Receive Response from Server in Time? 3-52
Appendix A Description of RAS Installation Directory A-1
Appendix B Description of RAC Installation Directory B-1

Part 3 Appendix

Table of Contents i
Appendix A Glossary A-1
Appendix B Acronyms and Abbreviations B-1

Index .....

HUAWEI

1. SysPatron System Patron

2. iWeb Remote Maintenance Access System

U-SYS SoftX3000 SoftSwitch System

BAM User Manual

V300R003

Huawei Technologies Proprietary

U-SYS SoftX3000 SoftSwitch System

BAM User Manual

Manual Version	T2-010145-20050331-C-3.30
Product Version	V300R003
BOM	31015045

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd.,

Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: http://www.huawei.com

Email: support@huawei.com

Copyright © 2005 Huawei Technologies Co., Ltd.

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks

, HUAWEI, C&C08, EAST8000, HONET, , ViewPoint, INtess, ETS, DMC, TELLIN, InfoLink, Netkey, Quidway, SYNLOCK, Radium, M900/M1800, TELESIGHT, Quidview, Musa, Airbridge, Tellwin, Inmedia, VRP, DOPRA, iTELLIN, HUAWEI OptiX, C&C08 iNET, NETENGINE, OptiX, iSite, U-SYS, iMUSE, OpenEye, Lansway, SmartAX, infoX, and TopEng are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

About This Manual

Release Notes

The manual applies to the U-SYS SoftX3000 SoftSwitch System V300R003 (hereinafter referred to as the SoftX3000).

Related Manuals

The related manuals are listed in the following table.

Manual	Content
U-SYS SoftX3000 SoftSwitch System Technical Manual-System Description	It provides an overall introduction to the SoftX3000, including product features, applications, and technical specifications.
U-SYS SoftX3000 SoftSwitch System Technical Manual-System Principle	It details on the hardware architecture, component interworking mechanism, and subsystems of alarm, billing, and clock in the SoftX3000.
U-SYS SoftX3000 SoftSwitch System Hardware Description Manual	It details the features and technical specifications of the hardware components of the SoftX3000, including cabinets, frames, boards, cables, and cabinet internal components.
U-SYS SoftX3000 SoftSwitch System Technical Manual–Services and Features	It covers various services and functions supported by the SoftX3000, including voice services, supplementary services, IP Centrex services, multi-media services, value added services, dual homing functions, charging functions, IPTN functions, remote network access functions, and so on.
U-SYS SoftX3000 SoftSwitch System Hardware Installation Manual	It details the installation procedure of the SoftX3000 hardware components, and matters needing attention during the installation process.
U-SYS SoftX3000 SoftSwitch System Software Installation Manual	It covers the detailed procedure of installing the SoftX3000 software, including BAM server, emergency workstation, and client, focusing on the key points that might cause installation failure.
U-SYS SoftX3000 SoftSwitch System Routine Maintenance Guide	It guides the maintenance engineers to perform daily maintenance, monthly maintenance, and yearly maintenance tasks on the SoftX3000.

Manual	Content
U-SYS SoftX3000 SoftSwitch System Emergency Maintenance Manual	It guides the maintenance engineers to perform recovery operations in the case of emergencies, such as congestion of global service, AMG, and TMG, and failure of host and BAM.
U-SYS SoftX3000 SoftSwitch System Part Replacement Guide	It guides the maintenance engineers on how to replace hardware components of the SoftX3000, such as boards, fan frame, LAN Switch, and hard disk.
U-SYS SoftX3000 SoftSwitch System Operation Manual-Configuration Guide	It guides the engineers how to configure various data in the SoftX3000, including configuration steps, preparations, database table referencing relationships, and command parameters.
U-SYS SoftX3000 SoftSwitch System Operation Manual-Configuration Examples	It guides the engineers how to configure various data in the SoftX3000, including networking example, configuration script, key parameters and debugging guidance.
U-SYS SoftX3000 SoftSwitch System Operation Manual-Performance Measurement	It guides the engineers how to work on performance measurement tasks and analyze measurement results.
U-SYS SoftX3000 SoftSwitch System Operation Manual-GUI Guide	It guides the engineers how to use the GUI on various clients of the SoftX3000, including operations on menus and navigation tree. In addition, it introduces the operations on TableBrowse.
U-SYS SoftX3000 SoftSwitch System BAM User Manual	It guides the engineers how to install and use the software related to the BAM, including remote maintenance software, anti-virus software, system customized software, and so on.
U-SYS iGateway Bill User Manual	It elaborates on the functioning principle of the iGateway Bill. Also, it teaches you on how to install, maintain, and operate the product.

Organization

The manual presents the principle, installation, operation, and maintenance of the two BAM components in the following structure.

The manual contains two sections:

- **01-SysPatron System Patron** introduces the features, installation procedures, operation guidances, and FAQs on the SysPatron System Patron.

- **02-iWeb Remote Maintenance Access System** details the features, installation procedures, operation guidance, and FAQs on the iWeb Remote Maintenance Access System.
- **Appendix** lists the glossary, acronyms and abbreviations used in the manual.

Intended Audience

The manual is intended for the following readers:

- NGN network planning experts
- NGN network administrators
- NGN system engineers

Conventions

The manual uses the following conventions::

I. General conventions

Convention	Description
Arial	Normal paragraphs are in Arial.
Boldface	Headings are in **Boldface**.
`Courier New`	Terminal Display is in `Courier New`.

II. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click the <OK> button.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

III. Keyboard operation

Format	Description
<Key>	Press the key with the key name inside angle brackets. For example, <Enter>, <Tab>, <Backspace>, or <A>.

Format	Description
<Key1+Key2>	Press the keys concurrently. For example, <Ctrl+Alt+A> means the three keys should be pressed concurrently.
<Key1, Key2>	Press the keys in turn. For example, <Alt, A> means the two keys should be pressed in turn.

IV. Mouse operation

Action	Description
Click	Press the left button or right button quickly (left button by default).
Double Click	Press the left button twice continuously and quickly.
Drag	Press and hold the left button and drag it to a certain position.

V. Symbols

Eye-catching symbols are also used in the manual to highlight the points worthy of special attention during the operation. They are defined as follows:

⚠ **Caution**, **Warning**, **Danger**: Means reader be extremely careful during the operation.

🕮 **Note**, **Comment**, **Tip**, **Knowhow**, **Thought**: Means a complementary description

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

HUAWEI

U-SYS SoftX3000 SoftSwitch System
BAM User Manual

Part 1 SysPatron System Patron

Table of Contents

Chapter 1 System Description 1-1
1.1 Overview of System SysPatron 1-1
1.2 Comparing with Ordinary Anti-Virus Software 1-1
1.2.1 Features of Ordinary Anti-Virus Software 1-1
1.2.2 Features of SysPatron 1-1
1.2.3 Comparison Results 1-1
1.3 Function Description 1-2
1.3.1 Overview of SysPatron Functions 1-2
1.3.2 System Verification 1-3
1.3.3 Progress Monitoring 1-4
1.3.4 Integrity Detection 1-5
1.3.5 Log Management 1-5
1.3.6 Alarm Management 1-6
1.4 Software and Hardware Configuration 1-6
1.4.1 Hardware Configuration 1-6
1.4.2 Software Configuration 1-7

Chapter 2 Installing System SysPatron 2-1
2.1 Precautions 2-1
2.2 Software Installation 2-2
2.2.1 Installation Flow 2-2
2.2.2 Preparations Before Installation 2-2
2.2.3 Installation Process 2-3
2.2.4 Installation Check 2-6
2.3 Uninstalling Software 2-8

Chapter 3 Basic Operations 3-1
3.1 Overview of Basic Operations 3-1
3.2 Generating Verification Files 3-1
3.2.1 Selecting Source Files 3-1
3.2.2 Generating Verification Files 3-2
3.3 Starting SysPatron 3-2
3.4 Stopping the SysPatron Processes 3-3
3.5 Checking the System Integrity 3-4
3.6 Checking and Processing the Alarm 3-5
3.7 Checking Log File 3-7

Chapter 4 FAQs 4-1
4.1 Overview of FAQs 4-1
4.2 Installation Terminated at License Agreement 4-1

4.3 SysPatron Cannot be Started 4-1
4.4 How to Change the Startup Type of _UM_PPT_Service_ 4-1
4.5 Need Verification Files for Commonly Used Programs? 4-2
4.6 Edit Registry Items of SysPatron? 4-2
4.7 Cannot Access Files or Use Applications After Installing SysPatron 4-2
4.8 SysPatron Still Functions After Uninstallation 4-2
4.9 SysPatron Cannot Be Reinstalled After Uninstallation 4-3

Appendix A Description of Installation Folders A-1

Appendix B Description of Configuration File B-1
B.1 Editing Description of Configuration File B-1
B.2 Description of Parameter Segments B-2
B.2.1 Overview of Parameter Segments B-2
B.2.2 Core File List [PROCESSES] B-2
B.2.3 Detection File List [FILES] B-6
B.2.4 Timing Detection Parameter [BASIC] B-7
B.2.5 Log Management Parameter [BASIC] B-9
B.2.6 Alarm Parameter [WARNING] B-11

Chapter 1 System Description

1.1 Overview of System SysPatron

As a bridge between telecommunication equipments and the operation network, a server is a weak link for security management. One is that Window 2000 Server used in a server is likely to be a channel for illegal attack due to its safety problem. The other is that out of service needs, third-party software has to be installed in a server, increasing the possibility of its virus infection. Therefore, one telecom operators' deep concern is how to enhance the anti-virus capacity of a server and network security.

Thereby, Huawei Technologies Co., Ltd. developed the i3 SURE SysPatron system patron (hereinafter referred to as "SysPatron"). The SysPatron is intended for enhancing the virus detection and resistance capacities of a server which uses Windows 2000 Server as operating system platform.

1.2 Comparing with Ordinary Anti-Virus Software

1.2.1 Features of Ordinary Anti-Virus Software

At present, most of anti-virus products detects and resists viruses in the code comparison mode. The processing flow is:

1) Compare source codes in a program or a file with virus attributes in a virus database.
2) Confirm whether the program or the file is infected based on the result.
3) Report exception process alarm, and prohibit program automatic running
4) Restore and delete the infected file.

1.2.2 Features of SysPatron

Unlike ordinary anti-virus software, which are designed to scan and kill viruses in the system, the SysPatron

1.2.3 Comparison Results

Table 1-1 Comparison between ordinary anti-virus software and SysPatron

Features	SysPatron	Other software
Usability	Simple and easy to use	Comprehensive and hard to use
Effect on the system	Major	Minor
Upgrade frequency	Not frequently	Periodic

Features	SysPatron	Other software
Can kill virus	No	Yes
Range of usage	Specific	Universal

These anti-virus products have the following features:

Comprehensive functions and have a small effect on Windows operating system program and other application programs.

The weak points are that their virus databases must be upgraded periodically and are not available to the latest viruses; also the products do not provide customized interfaces. These products are more suitable for individuals or enterprises for the non-dedicated purposes.

However, the SysPatron can detect and resist viruses through file verification and customized start. You first use the SysPatron to verify normal programs and files so as to generate verification files. After the start of the SysPatron, the SysPatron conducts 24-hour uninterrupted monitoring for the server progress and verifies the WIN32 that requests for operation in real time. If real-time verification results and verification files are inconsistent, the SysPatron sends an alarm and determines whether to disable the program based on the system configuration. Besides, the SysPatron can check the integrity for designated programs or files to find viruses and prevent them from spreading timely.

Its strong points are that with the easy operation and maintenance, it is not upgraded frequently; it can resist latest viruses and provide customized interfaces, abundant logs and alarms. Its weak points are that it cannot kill viruses without cooperating with other tools; it affects the usage of other application programs to some extent (For example, undefined programs cannot run in the configuration file). Compared with other anti-virus products, the SysPatron is more suitable for dedicated applications.

1.3 Function Description

1.3.1 Overview of SysPatron Functions

The SysPatron mainly provides the following five functions:

- System verification
- Progress monitoring
- Integrity detection
- Alarm management
- Log management

1.3.2 System Verification

The core file list and the detection file list are two important parameter segments in the system configuration file ppt.ini. The former defines the WIN32 programs enabled on the server, such as operating system programs and important application programs. The latter includes other important programs and files that need checking periodically. For details, refer to the related part in “Appendix B Description of Configuration File” in this manual.

Usually, verification files must be generated and saved properly for programs and files in both the core file list and the detection file list because these verification files are the basis of process monitoring and integrity detection. Each source file corresponds to a verification file which name is “<source file name>_<source file extension name>_PPT_“. For example, the source file test.exe corresponds to the verification file test_exe._PPT_.

A verification file can be generated in the following two ways:

I. Automatic Generation During the Installation of the SysPatron

During the installation of the SysPatron, the default core file list and the default detection file list are generated automatically. Verification files are also generated automatically for programs and files in the lists to ensure the normal running of the operating system and server software after the installation. Automatically-generated verification files and source files must be under the same directory.

II. Generation by Tool After the Installation of the SysPatron

The SysPatron provides a special tool VerifyFileCreator.exe to verify files and file lists and then to generate verification files. For details, refer to “3.1 Generating Verification Files”.

Cautions:

Before the generation of verification files, make sure that source files are normal. Otherwise, the verification is meaningless.

For a newly-installed server, it is recommended that verification files are generated immediately after the installation of basic software (operating system software and server software), so as to avoid the virus infection due to the online running of source files and the use of other software.

For the server with a certain running period, it is recommended that other tools are used to kill viruses first and then verification files are generated.

1.3.3 Progress Monitoring

Through monitoring the progress, the SysPatron can control programs and services running on the server so as to prevent viruses from attack. Its process monitoring flow is shown in Figure 1-1.

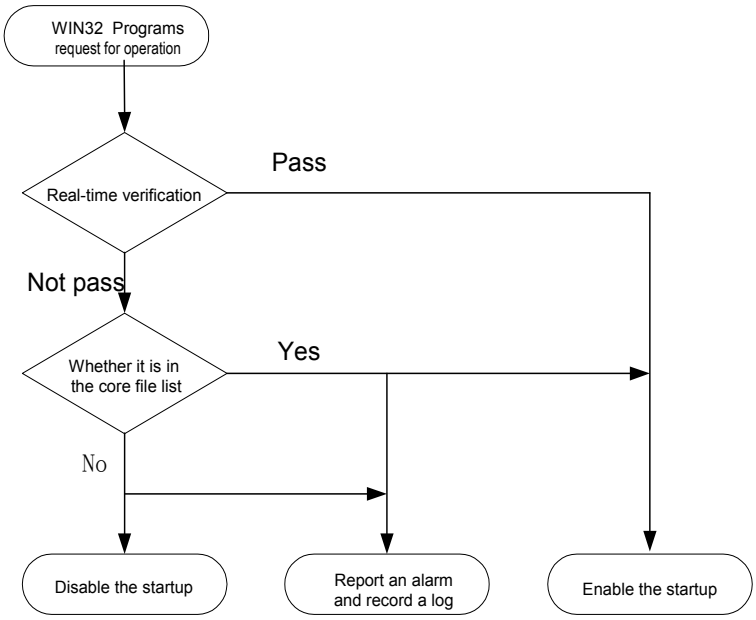


Figure 1-1 Flow of progress monitoring

As shown in the above figure, the core content of the progress monitoring is the real-time verification. The specific steps of the real-time verification are shown as below:

1) Check whether verification files exist and their formats are correct.
2) Retrieve file sizes in verification files; compare them with the current source file sizes to check whether source files have changed.
3) Retrieve the data of source files and generate verification data based on algorithm.
4) Compare the verification data with the data in verification files to check whether source files have changed.

After the completion, the SysPatron takes the related handling measures based on verification results and specific configuration.

- If verification files exist, their formats are correct, and their data is consistent, the real-time verification is passed. The SysPatron enables the WIN32 programs.
- If not, the real-time verification is not passed. The SysPatron determines whether to enable WIN32 programs based on the configuration of the core file list. For undefined WIN32 programs in the core file list, the SysPatron disables their running. Meanwhile, it generates an alarm and records the problem in the log. For

defined WIN32 programs in the core file list, the SysPatron enables their running. Also it generates an alarm and records the problem in the log.

1.3.4 Integrity Detection

Integrity detection means the SysPatron verifies programs or files in the core file list and the detection file list and confirms these programs or files are normal. Its steps are the same as those of the real-time verification, but the processes following their verifications are different.

- If the integrity detection is passed, programs and files are normal and the SysPatron does not conduct any process.
- If not, programs and files may be infected by viruses. The SysPatron generates an alarm and records the problem in the log.

The integrity detection can be implemented by manual detection and timing detection.

I. Manual Detection

Manual detection means you can use a support tool to detect the system integrity. For details about it, refer to the related part in “3.4 Checking System Integrity“.

II. Timing Detection

Timing detection means the SysPatron detects the integrity periodically based on the setting in the configuration file ppt.ini. Through it, maintenance personnel can find and delete viruses timely. For the setting of timing detection parameters, refer to “Timing Detection Parameters” in “Appendix B Description of Configuration File”.

Note:

- If the SysPatron stops running, the timing detection also stops running.
- If timing detection parameters are not configured or the SysPatron fails to obtain timing detection parameters, the SysPatron executes the detection based on the default parameter values.

1.3.5 Log Management

Log management includes log write and log file automatic backup.

The SysPatron records some related log information during its running. For example, when the SysPatron carries out verifications, verification failure or termination are recorded in the log. The log file is a text file; the default file name is ppt.log which is created automatically during the installation and stored under the installation directory of the SysPatron.

If the size of the log file exceeds the set maximum value, the SysPatron backs up the log file under a designated log backup directory automatically and clears log files automatically that has been saved for a long period. You can set such parameters as the log file size, log backup file path and maximum date saved in the configuration file ppt.ini. For details, refer to “Log Management Parameters” in “Appendix B Description of Configuration File”

The format of a log can be divided into three parts: the first part is the data and the time of the log; the second part is the name of the functional module that leads to the log; the third part is the specific content of the log.

```
2004-09-25  18:25:03        System monitor        Starting system monitor.
```

1.3.6 Alarm Management

Based on alarm information formats set in the configuration file ppt.ini, the SysPatron sends alarms to the SoftX3000 through invoking alarm functions in the alarm interface file WarnIn.dll. SoftX3000 displays the alarm information in the alarm windows of the alarm console and maintenance console.

Caution:

If there is no WarnIn.dll file under the installation directory of the SysPatron, the SysPatron cannot send alarm information. Therefore, do not delete the file WarnIn.dll.

1.4 Software and Hardware Configuration

1.4.1 Hardware Configuration

The running of the server must meet the following requirements for hardware configuration.

- CPU(Center Processing Unit): Pentium 133 MHz or above.
- RAM (Random Access Memory):128 M or above.
- Hard disk: The disk space depends on the system setting and actual running condition and meets the requirements of the installation of the SysPatron, log and backup.
- Network card: It is installed and can be used normally.

Note:

- The space of the disk where the installation directory is located must be larger than the actual need, so as to ensure that the log information can be recorded normally.
- The space of the disk where the log file backup directory is located depends on the actual running condition of the SysPatron. If exceptions occur frequently, the disk space must be more larger so as to ensure the normal log backup.

1.4.2 Software Configuration

I. Software Composition of the SysPatron

The SysPatron is not an individual program, but a software system made up of several programs and files. Its system can be divided into three parts: core application file, files, support tools. For details, refer to “Appendix A Description of Installation Directory”.

II. Matched Software

At present, the operating system platform matching with the SysPatron is Windows 2000 Server. No other matched software is required.

Chapter 2 Installing System SysPatron

2.1 Precautions

Pay attention to the following precautions during the installation of the SysPatron.

- Different products use different versions of SysPatrons. The automatically-generated core file lists and alarm information of different editions are inconsistent completely. If you use a SysPatron matching with other products, the server cannot work normally. Therefore, be sure to install the SysPatron delivered with the SoftX3000.
- The installation of the SysPatron must follow the sequence described in this manual. Or the system may work abnormally as a result.
- The SysPatron runs automatically after the installation, so you need not restart the computer.
- The SysPatron does not provide upgrade function. You can upgrade it by uninstalling the old edition and installing a new edition.
- After starting the SysPatron, you cannot install the commonly used software normally because of the system monitoring function. In this case, the software installation can be finished only when you close the SysPatron. Such an operation may bring out security problem. Also, you have to generate the verification files of these software manually. Therefore, you should install commonly used software before installing the SysPatron.
- At present, the default core file list only includes the related programs of operating system and BAM server software. After the installation, check the configuration file ppt.ini timely. Based on the actual needs, supplement the core file list and modify other important parameters such as timing detection parameters, log backup parameters.

Caution:

If you modify the contents in the system configuration file (especially the core file list), the security performance of the server may be affected directly. Be cautious with this operation.

After the configuration file is modified, you need not to restart the SysPatron.

2.2 Software Installation

2.2.1 Installation Flow

The installation flow of the SysPatron is shown in Figure 2-1.

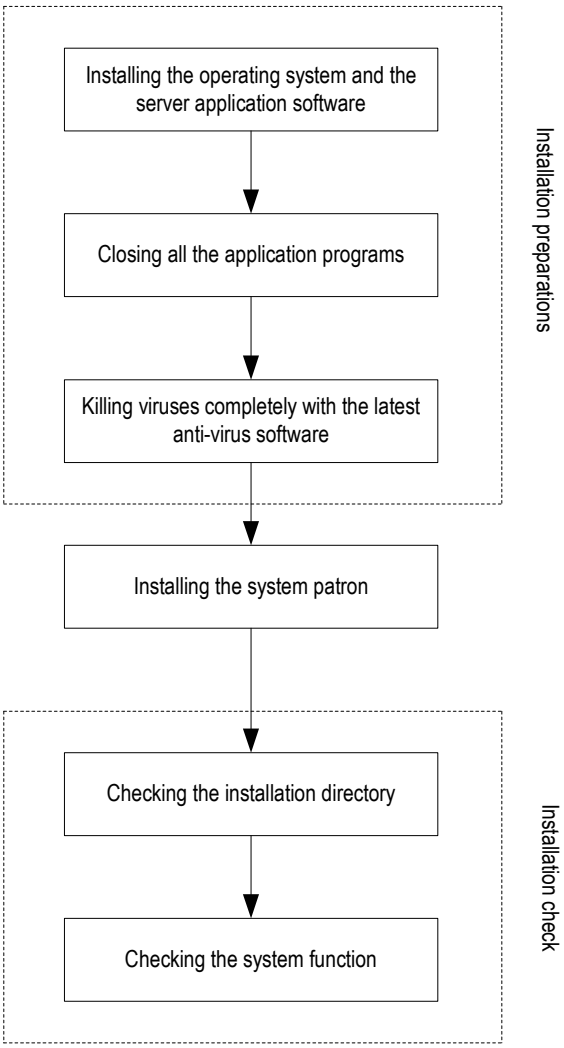

Installing the operating system and the server application software
Closing all the application programs
Killing viruses completely with the latest anti-virus software
Installing the system patron
Checking the installation directory
Checking the system function
Installation preparations
Installation check

Figure 2-1 Installation flow of the SysPatron

2.2.2 Preparations Before Installation

Before the installation of the SysPatron, you must prepare the following.

I. Installing the operating system and the server application software

At present, the SysPatron only can run on the Windows 2000 Server operating system. Therefore, you must install it on the server. Moreover, before the installation, you should install server software, database software and tool software required on the

server. For the installation of the Windows 2000 Server and other application software, refer to *U-SYS SoftX3000 Softswitch System Installation Manual Software Installation* .

II. Closing All Application Programs

Closing all the application programs can prevent their running from affecting the installation of the SysPatron. Also it can avoid some viruses in the memory from being omitted before the installation.

III. Killing Viruses Completely by Latest Anti-Virus Software

To generate verification files correctly, use the latest anti-virus software to protect against viruses completely before the installation of the SysPatron. The online anti-virus scan mode can only kill viruses in files, and its speed is slow. It is recommended that you start up a compact disk or a floppy disk to kill viruses.

Note:

Full anti-virus scan not only includes the anti-virus scan for the hard disk, but also the check for the memory and the creation of the system firewall.

2.2.3 Installation Process

To install the SysPatron, process as below:

1) Run the Setup.exe program in the installation disk of the SysPatron.
2) The window "Software Licensing Agreement" opens, as shown in Figure 2-2.

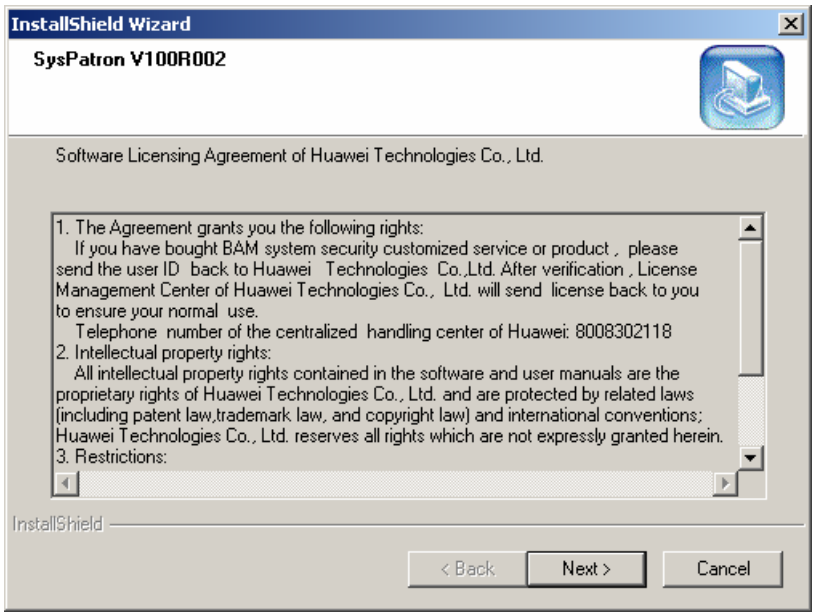

InstallShield Wizard
SysPatron V100R002
Software Licensing Agreement of Huawei Technologies Co., Ltd.
1. The Agreement grants you the following rights:
If you have bought BAM system security customized service or product , please send the user ID back to Huawei Technologies Co.,Ltd. After verification , License Management Center of Huawei Technologies Co., Ltd. will send license back to you to ensure your normal use.
Telephone number of the centralized handling center of Huawei: 8008302118
2. Intellectual property rights:
All intellectual property rights contained in the software and user manuals are the proprietary rights of Huawei Technologies Co., Ltd. and are protected by related laws (including patent law,trademark law, and copyright law) and international conventions; Huawei Technologies Co., Ltd. reserves all rights which are not expressly granted herein.
3. Restrictions:
InstallShield
< Back
Next >
Cancel

Figure 2-2 ”Software Licensing Agreement” window

3) Click <Next>.

4) The window "License Verification" opens, as shown in Figure 2-3.

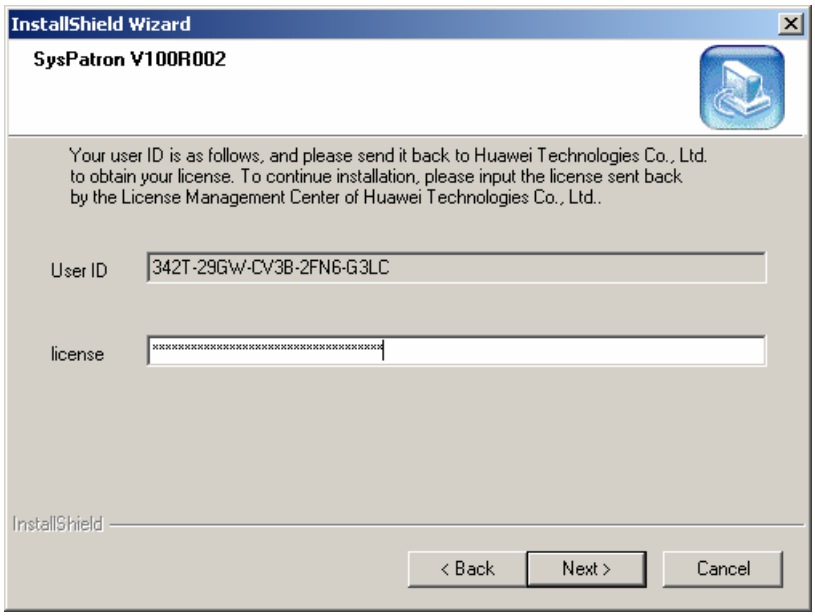

InstallShield Wizard
SysPatron V100R002
Your user ID is as follows, and please send it back to Huawei Technologies Co., Ltd. to obtain your license. To continue installation, please input the license sent back by the License Management Center of Huawei Technologies Co., Ltd..
User ID
342T-29GW-CV3B-2FN6-G3LC
license
InstallShield
< Back
Next >
Cancel

Figure 2-3 “License Verification" window

5) To obtain the license code corresponding to the user flag code, you should send the user flag code to License management center of Huawei, and then input the correct license code in the "license" field. If the input license code is not correct, you cannot install the SysPatron.

6) Click <Next>. The window "Choose Destination Location" opens, as shown in Figure 2-4.

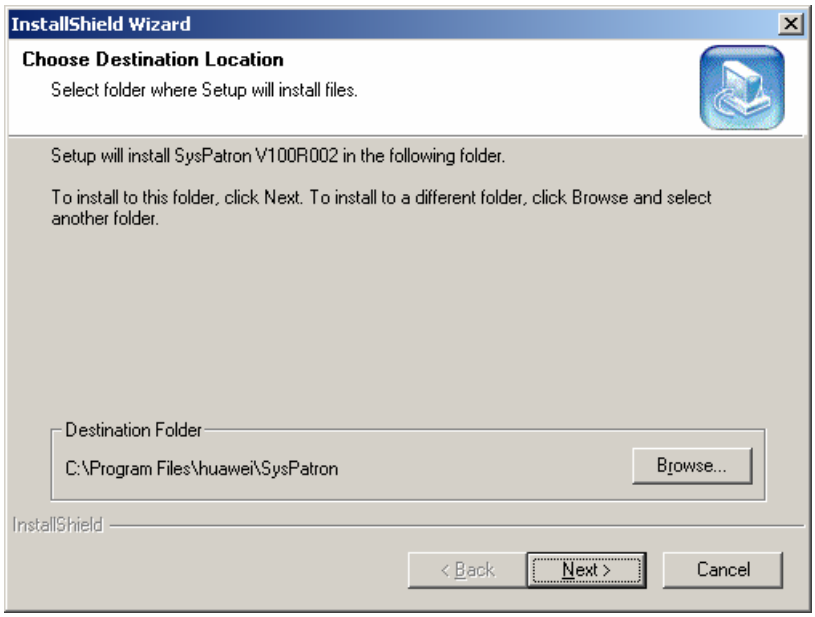

InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install SysPatron V100R002 in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\huawei\SysPatron
Browse...
InstallShield
< Back
Next >
Cancel

Figure 2-4 “Choose Destination Location” window

By default, the installation directory of the SysPatron is C:\Program Files\huawei\SysPatron. You can also select another directory as the installation directory through clicking <Browse>. It is recommended to adopt the default value of the system.

7) Click <Next>.

8) The window "Start Copying Files" opens, as shown in Figure 2-5.

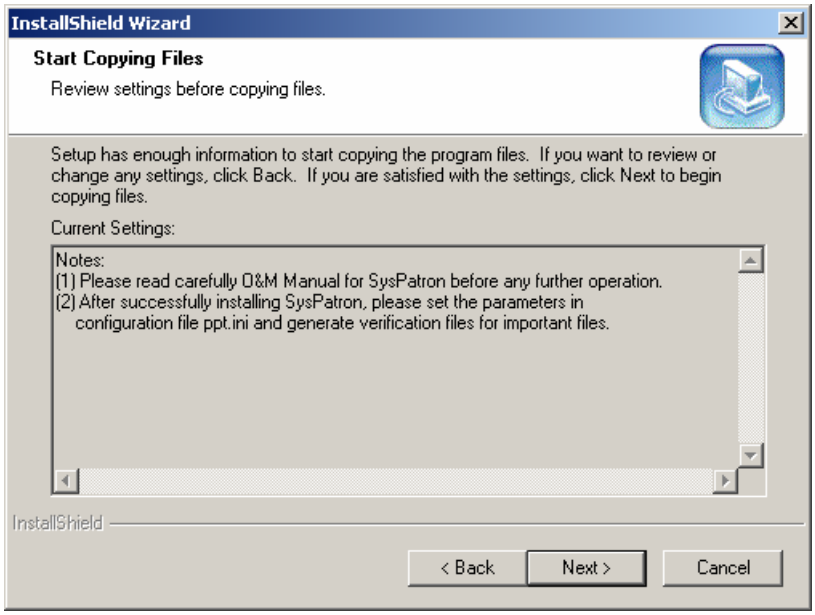

InstallShield Wizard
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Notes:
(1) Please read carefully O&M Manual for SysPatron before any further operation.
(2) After successfully installing SysPatron, please set the parameters in configuration file ppt.ini and generate verification files for important files.
InstallShield
< Back
Next >
Cancel

Figure 2-5 “Start Copying Files” window

9) Click <Next>.

The system starts copying files to the installation directory, and then the “InstallShield Wizard Complete" window pops up, as shown in Figure 2-6.

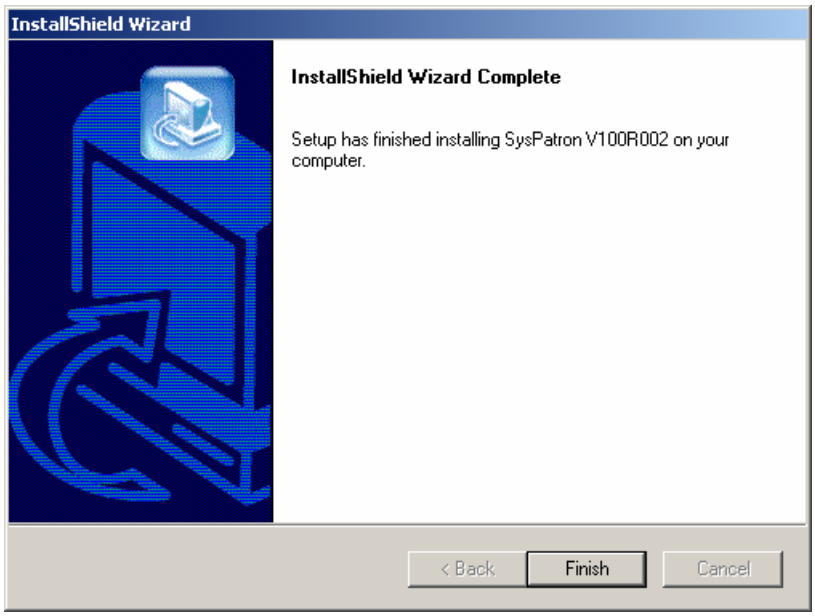


Figure 2-6 "InstallShield Wizard Complete" window

10) Click <Finish>.

The system first prompts "Syspatron has been installed successfully" and then displays "Syspatron has been started successfully". By now, the SysPatron generates verification files for programs and files in the core file list and the detection file list, and starts progress monitoring and time detection.

2.2.4 Installation Check

After the installation, check the installation result to ensure that the SysPatron can work normally. The check includes the following two items.

I. Check for the Installation Directory

The main purpose of the check is to confirm whether the installation directory of the SysPatron is complete. For details, refer to "Appendix A Description of Installation Directory".

II. Check whether the menu item of the SysPatron exists

After the installation, the menu item [SpyControl] appears in the menu [Start/Programs].

III. Check whether the SysPatron is started normally

After the installation, the SysPatron service (_UM_PPT_Service) is added to the system service list automatically and then is started. Select [Start/Programs/Administrative Tools/Services] to enter the window "Services". Then check whether the _UM_PPT_Service_ exists and is started. If yes, it indicates the SysPatron is installed normally, as shown in Figure 2-7.

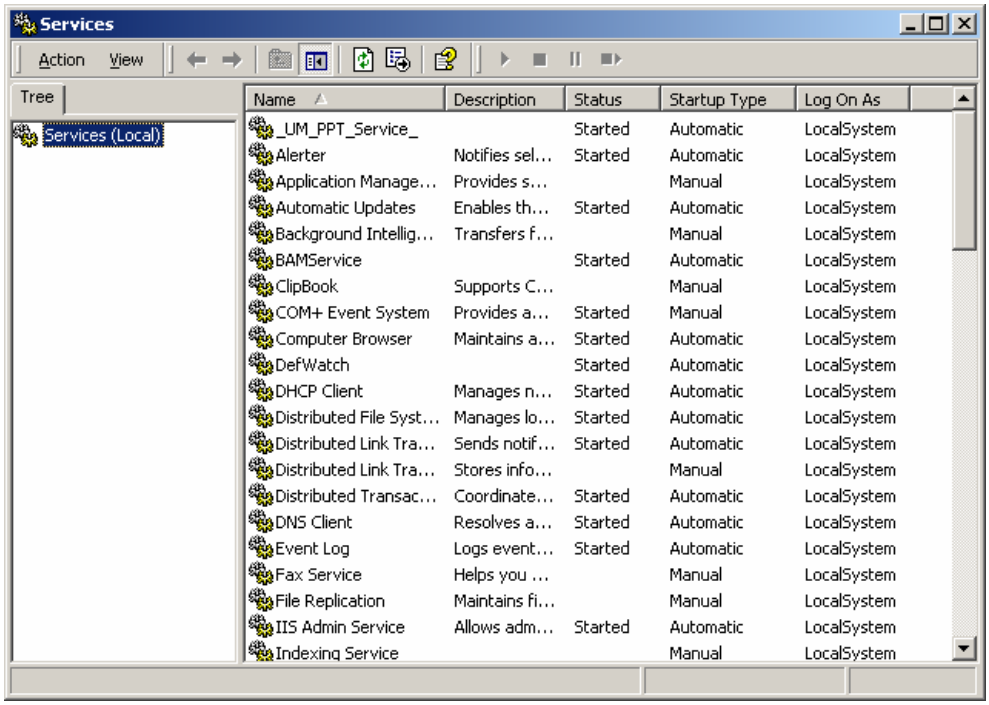

Services
Action View
Tree
Services (Local)
Name Description Status Startup Type Log On As
_UM_PPT_Service_ Started Automatic LocalSystem
Alerter Notifies sel... Started Automatic LocalSystem
Application Manage... Provides s... Manual LocalSystem
Automatic Updates Enables th... Started Automatic LocalSystem
Background Intellig... Transfers f... Manual LocalSystem
BAMService Started Automatic LocalSystem
ClipBook Supports C... Manual LocalSystem
COM+ Event System Provides a... Started Manual LocalSystem
Computer Browser Maintains a... Started Automatic LocalSystem
DefWatch Started Automatic LocalSystem
DHCP Client Manages n... Started Automatic LocalSystem
Distributed File Syst... Manages lo... Started Automatic LocalSystem
Distributed Link Tra... Sends notif... Started Automatic LocalSystem
Distributed Link Tra... Stores info... Manual LocalSystem
Distributed Transac... Coordinate... Started Automatic LocalSystem
DNS Client Resolves a... Started Automatic LocalSystem
Event Log Logs event... Started Automatic LocalSystem
Fax Service Helps you ... Manual LocalSystem
File Replication Maintains fi... Manual LocalSystem
IIS Admin Service Allows adm... Started Automatic LocalSystem
Indexing Service Manual LocalSystem

Figure 2-7 “Services”window

IV. Check whether verification files for programs and files in the file list are generated

Based on the core file list and the detection file list in the ppt.ini, you should check one by one whether verification files of various programs and files are generated. For the naming rule of verification files, refer to “1.1.2 System Verification”. If some verification files are not generated, you should use a support tool to generate them manually.

V. Check whether the system monitoring functions normally

Click an application program of a third-party software. Based on the actual conditions, the following results may occur.

- If the program is not listed in the core file list, the verification file exists and the verification is passed, you can use the program normally and no alarm is produced.
- If the program is not listed in the core file list, the verification file does not exist and the verification is not passed, you can use the program normally and there is an alarm prompt.
- If the program is listed in the core file list, the verification file is not generated and the verification fails, you can use the program normally and the verification is not passed on the alarm prompt.
- If the program is listed in the core file list, the verification file exists and the verification is passed, tyou can use the program normally and no alarm is produced.

VI. Check whether the timing detection function can be used normally

Use a support tool to generate verification files of programs and files manually based on the core file list and the detection file list in the configuration file ppt.ini. Meanwhile, set the timing detection mode as once every one hour. After a detection point, check the log file and alarm information. There should be no exceptions. Then, back up a verification file and then delete it or replace it with a wrong verification file. After another detection point, observe the log file and alarm information. There should be a prompt that the verification is not passed.

Note:

For manual generation operations of verification files, refer to “3.1 Generating Verification Files”.

For descriptions of timing detection parameters, refer to in “Timing Detection Parameters” in “Appendix B Description of Configuration File”.

After the detection, you should use backup files to replace deleted or modified verification files.

2.3 Uninstalling Software

You cannot uninstall the SysPatron during its running. Before the uninstallation, use the operating control and integrity detection tool SpyControl.exe to stop its running. The specific steps are shown as follows:

1) Select [Start/Programs/SpyControl] to enter the window “SpyControl”.

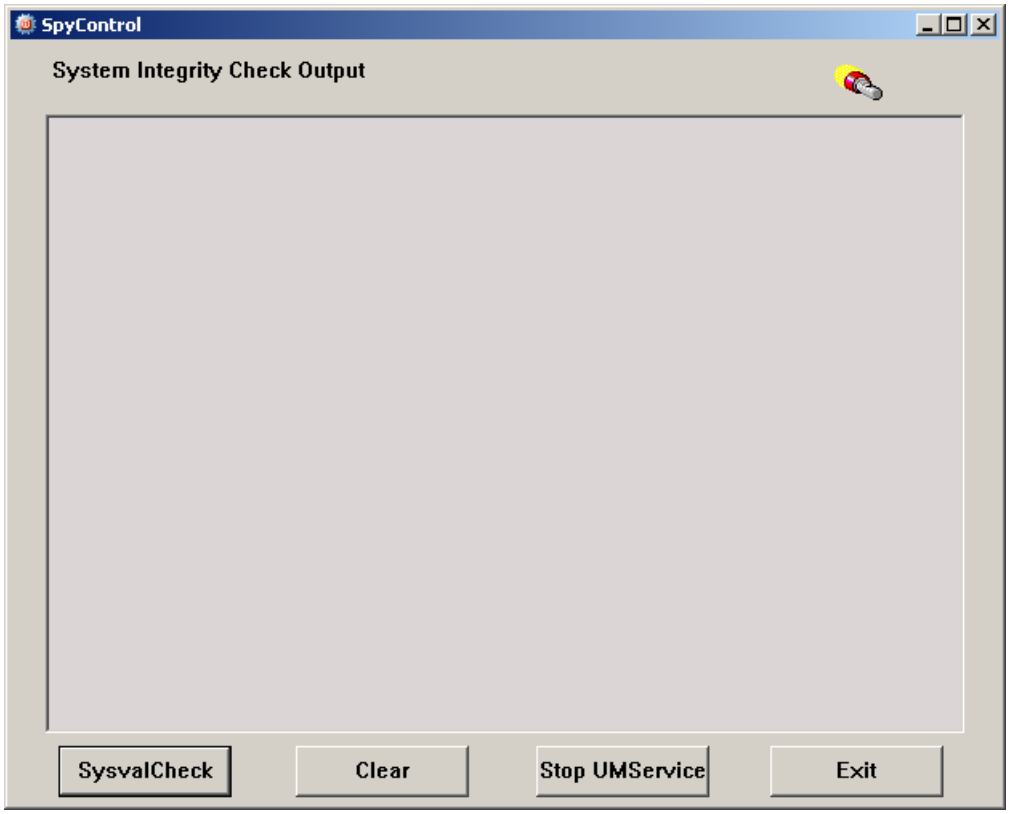


Figure 2-8 "SpyControl" window

2) Select <Stop UMService> to stop the running of the SysPatron.
3) Select [Start/Settings/Control Panel/ Add/Remove programs], and enter the window "Add/Remove programs", as shown in Figure 2-9.

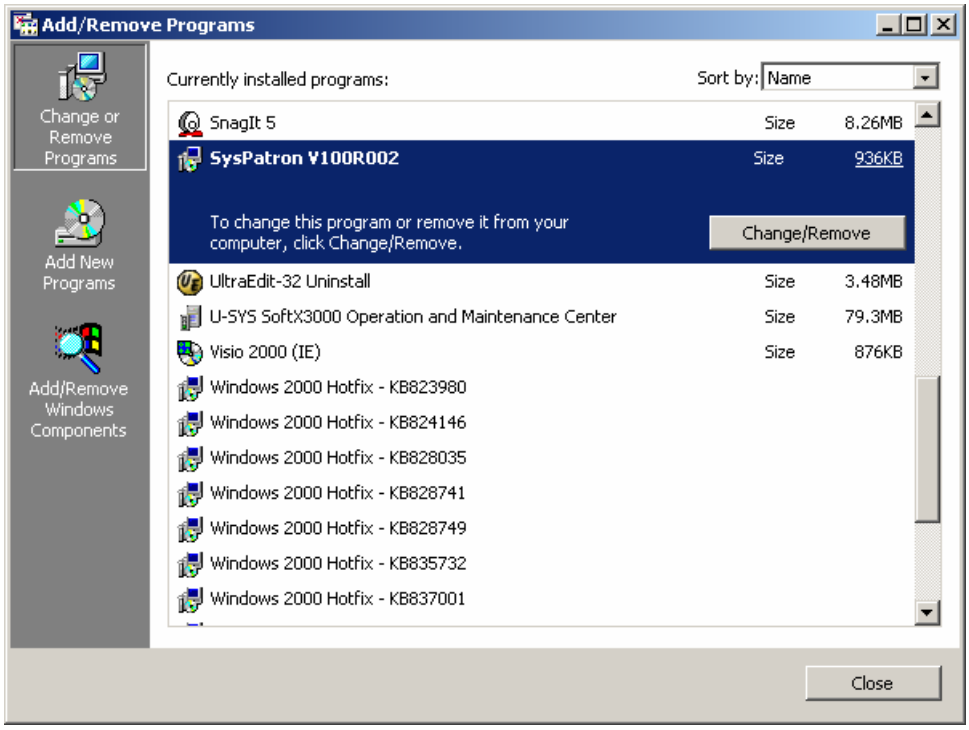

Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name
SnagIt 5 Size 8.26MB
SysPatron V100R002 Size 936KB
To change this program or remove it from your computer, click Change/Remove.
Change/Remove
UltraEdit-32 Uninstall Size 3.48MB
U-SYS SoftX3000 Operation and Maintenance Center Size 79.3MB
Visio 2000 (IE) Size 876KB
Windows 2000 Hotfix - KB823980
Windows 2000 Hotfix - KB824146
Windows 2000 Hotfix - KB828035
Windows 2000 Hotfix - KB828741
Windows 2000 Hotfix - KB828749
Windows 2000 Hotfix - KB835732
Windows 2000 Hotfix - KB837001
Close

Figure 2-9 "Add/Remove programs" window

4) Select "SysPatron VxxxRxxx", and click <Add/Remove>.
5) A prompt pops up, as shown in Figure 2-10. Click <Yes>.

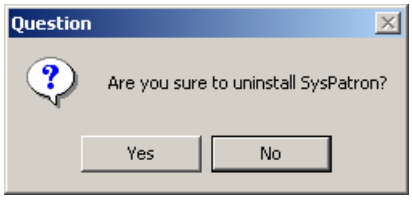


Figure 2-10 Prompt information of uninstalling the SysPatron

6) After the uninstallation, a prompt pops up, as shown in Figure 2-11.

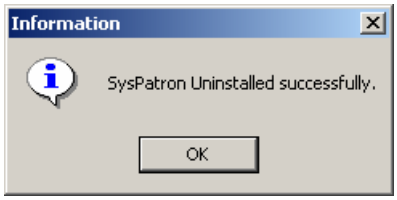


Figure 2-11 Prompt information of uninstallation finished

Click <OK>.

Chapter 3 Basic Operations

3.1 Overview of Basic Operations

The SysPatron itself has no operation interface. To start or close it, use a support tool. This chapter introduces the operations of support tools and the handling of logs and alarms.

3.2 Generating Verification Files

The SysPatron provides a special tool to generate verification files. The tool is under the installation destination directory of the SysPatron. Its file name is VerifyFileCreator.exe.

Run VerifyFileCreator.exe and then the window is shown in Figure 3-1.

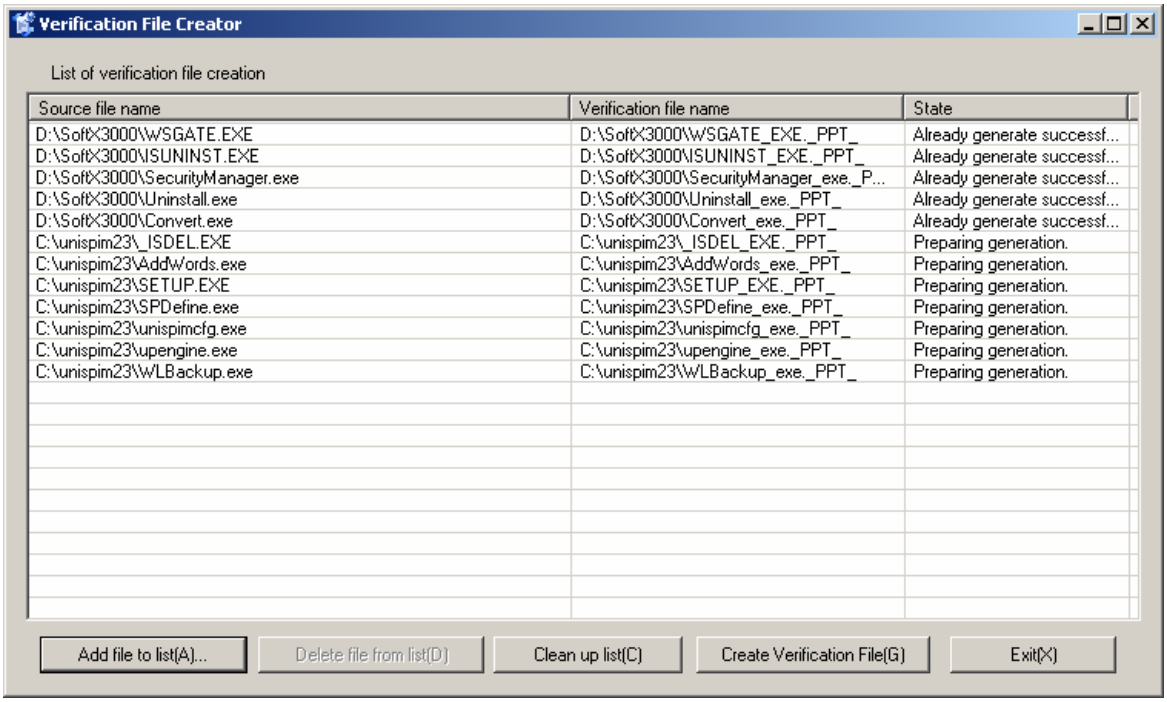


Figure 3-1 Generation tool of verification files

3.2.1 Selecting Source Files

By pressing the buttons in the above window, you can add, delete or clear up files in the list of verification file creation so as to confirm the source files that will generate verification files finally.

I. Adding a file to the list

Click <Add file to list>, and the dialogue box <Open> pops up. Select the file to be added. If the file to be added is not listed in the source file list, the generation tool of the verification file adds it to the end of the source file list automatically. Otherwise, the prompt that the file exists in the list appears.

II. Deleting a file from the list

To delete a line or multiple lines, select it in the file list and click <Delete file from list>, or press <Delete>.

III. Clearing up list

Click <Clear up list> and all the items are deleted from the list.

3.2.2 Generating Verification Files

After confirming the source files, click <Create Verification File>. The support tool helps to generate the verification files one by one for the source files in the list; the states (succeeded/failed) of the verification files are displayed in the list. if generating verification files fails, the following information is shown:

- New verification failed
- Write verification file failed
- Open file failed
- Read file failed
- Obtaining file size failed
- Naming verification file error
- Allocating memory failed
- Data coding failed
- Generating verification file succeeded

3.3 Starting SysPatron

Select [Start/Programs/SpyControl] to enter the window “SpyControl”. If the SysPatron is not started, the system monitoring button is displayed as <Start UMService> in the window. See Figure 3-2.

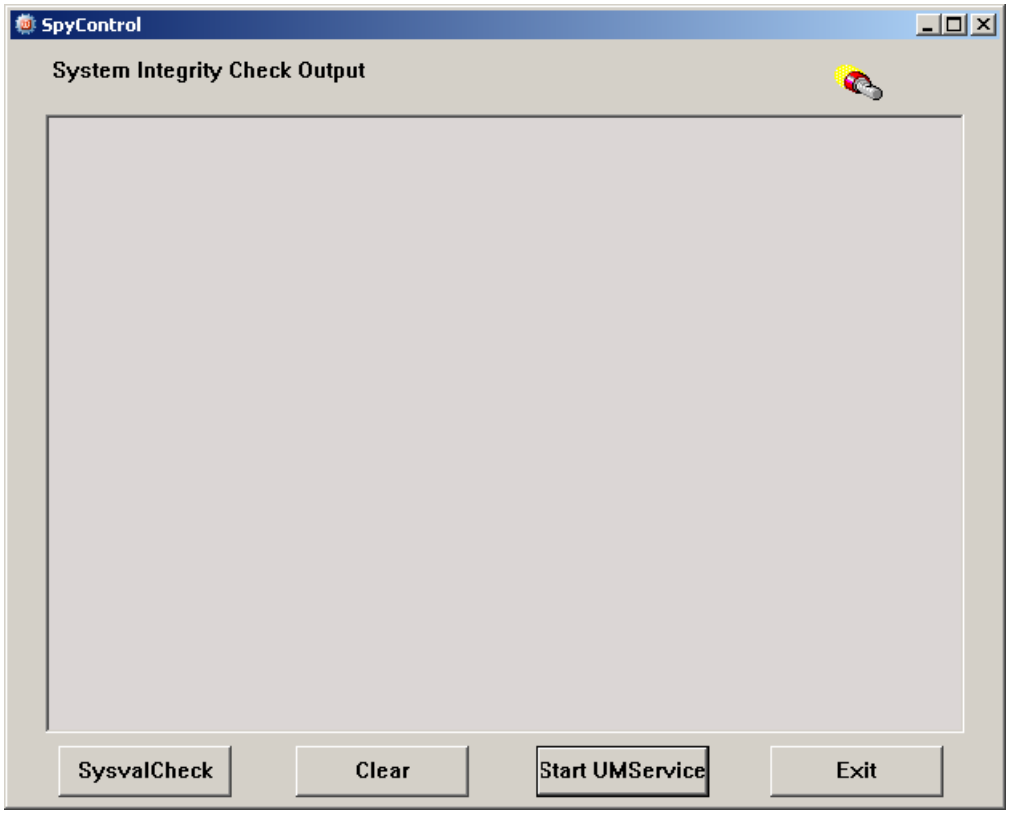


Figure 3-2 Starting the SysPatron

Click <Start UMService>. The SysPatron is started to carry out process monitoring, timing detection and alarm production.

3.4 Stopping the SysPatron Processes

Select [Start/Programs/SpyControl] to enter the window “SpyControl”. If the SysPatron is started, the system monitoring button at the low right of the window is displayed as <Stop UMService>. See Figure 3-3.

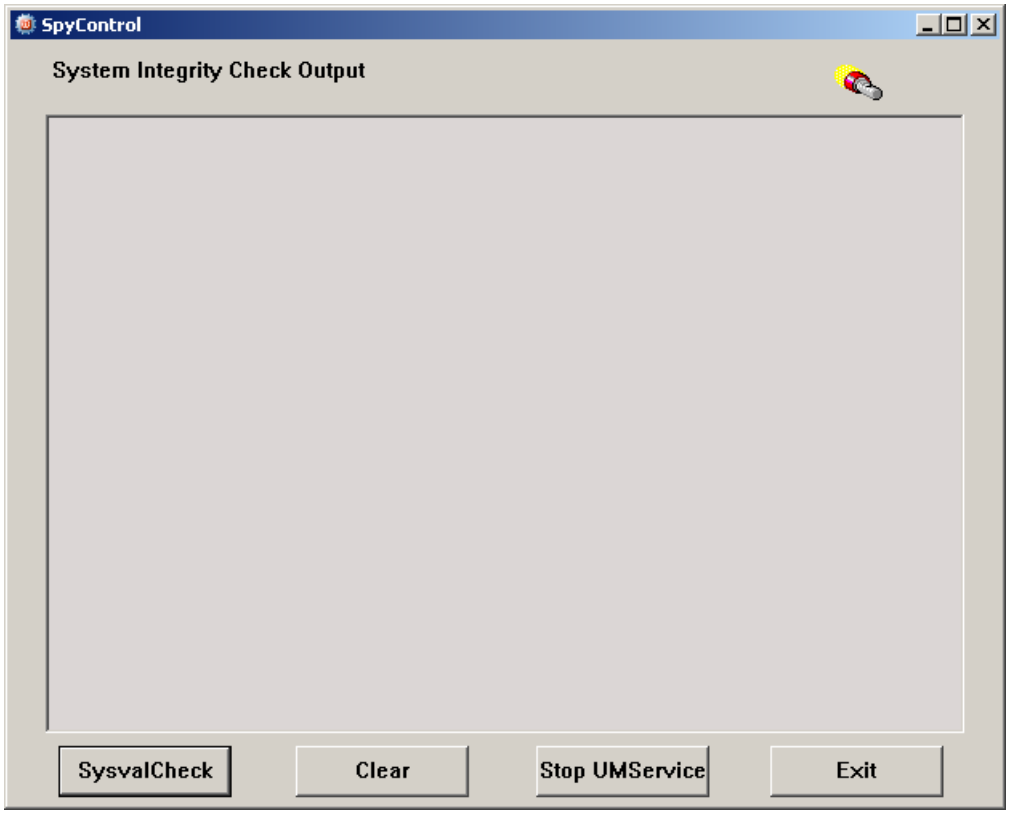


Figure 3-3 Closing the SysPatron

Select <Stop UMService>, and the operation results are either of the following:

- If the operation is successful, the window displays “System monitor has been stopped”.
- If the operation fails, the window displays “Can not close SysPatron”.

3.5 Checking the System Integrity

Select [Start/Programs/SpyControl] to enter the window “SpyControl”. Click <SysvalCheck> in the window to check programs and files in the core file list and the detection file list. The results exported after the check are shown in Figure 3-4.

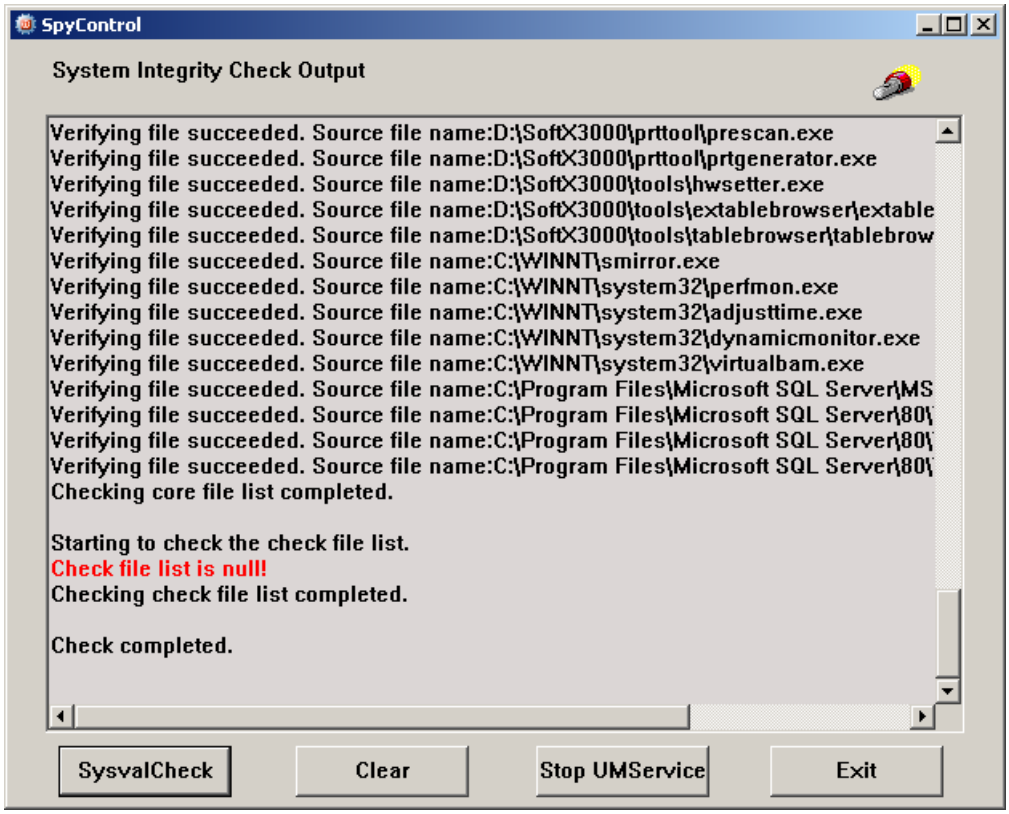

SpyControl
System Integrity Check Output
Verifying file succeeded. Source file name:D:\SoftX3000\prttool\prescan.exe
Verifying file succeeded. Source file name:D:\SoftX3000\prttool\prtgenerator.exe
Verifying file succeeded. Source file name:D:\SoftX3000\tools\hwsetter.exe
Verifying file succeeded. Source file name:D:\SoftX3000\tools\extablebrowser\extable
Verifying file succeeded. Source file name:D:\SoftX3000\tools\tablebrowser\tablebrow
Verifying file succeeded. Source file name:C:\WINNT\smirror.exe
Verifying file succeeded. Source file name:C:\WINNT\system32\perfmon.exe
Verifying file succeeded. Source file name:C:\WINNT\system32\adjusttime.exe
Verifying file succeeded. Source file name:C:\WINNT\system32\dynamicmonitor.exe
Verifying file succeeded. Source file name:C:\WINNT\system32\virtualbam.exe
Verifying file succeeded. Source file name:C:\Program Files\Microsoft SQL Server\MS
Verifying file succeeded. Source file name:C:\Program Files\Microsoft SQL Server\80\
Verifying file succeeded. Source file name:C:\Program Files\Microsoft SQL Server\80\
Verifying file succeeded. Source file name:C:\Program Files\Microsoft SQL Server\80\
Checking core file list completed.
Starting to check the check file list.
Check file list is null!
Checking check file list completed.
Check completed.
SysvalCheck
Clear
Stop UMService
Exit

Figure 3-4 Checking the system integrity

Click <Clear> in the “SpyControl” window. All the exported information in the window is cleared up.

Note:

- Do not carry out the system integrity detection when the system is busy.
- If verification files do not exist or verifications fail during the system integrity detection, the “Beep” tone is generated. Moreover, the alarm information in the red bold type is displayed in the “SpyControl” window.

3.6 Checking and Processing the Alarm

I. Common Alarm Information

At present, BAM anti-virus tool only produces the alarm “BAM file verify fail”. The specific alarm information is shown in Table 3-1.

Table 3-1 BAM antivirus tool alarm

Alarm name	BAM file verify fail
Alarm number	2320 (It means the alarm number in the SoftX3000)
Alarm type	Event alarm
Alarm level	Minor alarm
Alarm information	1) Name verify file error. 2) Open verify file fail. 3) Read verify file fail. 4) Invalid verify file. 5) Get size of verify file fail. 6) Open source file fail. 7) Read source file fail. 8) Get size of source file fail. 9) Source file size is not equal with the one stored in verify file head. 10) Memory allocate fail. 11) Data encode fail. 12) The verify code generate from source file is not equal to the one stored in verify file. 13) File verify succeed. 14) Source file not exists. 15) Verify file not exists.

II. Processing Programs or Files Infected

If you confirm that an program or file on the server is infected, proceed the following for processing.

1) Use the operating control and integrity testing tool to stop the running of the SysPatron.
2) If an infected program or file is running, close it first. If the operating system file is infected, restart the server with a compact disk or enter the safe mode.
3) Use antivirus software of the latest version to protect against the infected program or file. The online anti-virus mode can only kill viruses in files, and its speed is slow. It is recommended to use a compact disk or a floppy disk.
4) If you still cannot kill viruses, you can obtain an uninfected program or file from other sources and replace the infected program or file on the server. Note that both versions must be consistent.
5) After all the operations are finished, enable the system integrity detection function to check whether there are other infected programs. If yes, repeat steps from 1 to 4 until all the programs and files are recovered.
6) Restart the server.

3.7 Checking Log File

The log file records daily maintenance, operation and running status of the equipment. The common log information is shown in List 3-2.

Table 3-2 Common log information

Functional module	Content	Description
System monitor	Starting system monitor.	The SysPatron has been started.
Timing system integrity checker	Starting timing verification.	The integrity detection function of the SysPatron has been started.
System monitor	Verification file is inexistent. Source file name: …. Program hasn't been started.	The program has been defined in the core file list. Although its verification file does not exist and the system verification is not passed, the program is still started normally.
System monitor	Verification file is inexistent. Source file name: …. Program has been started.	The program has not been defined in the core file list. Because its verification file does not exist and the system check is not passed, the program fails to be started.
Timing system integrity checker	Check started.	Start timing detection.
Timing system integrity checker	Starting to check the core file list.	Start to check programs and files in the core file list.
Timing system integrity checker	Checking core file list completed.	Stop checking programs and files in the core file list.
Timing system integrity checker	Starting to check the check file list.	Start to check programs and files in the core file list.
Timing system integrity checker	Checking check file list completed.	Stop checking programs and files in the core file list.
Timing system integrity checker	Verification file is inexistent. Source file name: ….	Timing detection is not passed.
Timing system integrity checker	Stopping timing verification.	Disable integrity detection function
System monitor	Stopping system monitor.	Disable the running of the SysPatron

Chapter 4 FAQs

4.1 Overview of FAQs

In the use of the SysPatron, deal with the following problems that are met according to methods described in this manual. If you still cannot solve problems, contact Technical Support Department of Huawei.

4.2 Installation Terminated at License Agreement

During the installation, the window “Software Licensing Agreement” pops up. Click <Next>. The system prompts "Failed to basic files for setup…". The installation is terminated.

The cause is that the installation disk lacks the file “sptis.ix” or the file “sptia.ix_” has been damaged. Solution: Copy the normal file “sptia.ix_” to the installation disk.

4.3 SysPatron Cannot be Started

Proceed as follows:

1) In the installation directory of the SysPatron check whether the files “ProcActionSpy.sys” and “SpyCenter.exe” exist. If any of them is deleted, the SysPatron cannot be started. In this case, reinstall the SysPatron.
2) Select [Start/Programs/Administrative Tools/Services].
3) Check the state of _UM_PPT_Service_ in the "Service” window.
4) If the state of the _UM_PPT_Service_ is not “Started”, choose it and click the button on the tool bar to start the SysPatron.
5) If the system prompts the service _UM_PPT_Service_ cannot be started, restart the server.
6) If the SysPatron cannot be started after the restart of the server, the file ProcActionSpy.sys or SpyCenter.exe has been modified. The system patron must be reinstalled.

4.4 How to Change the Startup Type of _UM_PPT_Service_

If the startup type of the service _UM_PPT_Service_ is modified as “Manual”, what can be done to recover it as “automatic”?

Proceed as follows:

1) Select [Start/Programs/Administrative Tools/Services] to enter the window “Services”.
2) Right click the service _UM_PPT_Service_.

3) Select [Properties] in the shortcut menu.
4) Change the startup type to “Automatic”.

⚠ **Caution:**

If the startup type of the server is “Manual” or “Disabled”, change it to “Automatic”. Otherwise the operating system cannot work normally when you restart the computer.

4.5 Need Verification Files for Commonly Used Programs?

If the commonly used programs are added to the core file list, is it necessary to generate verification files for them?

It is better to generate verification files for these programs. Otherwise, the progress monitoring of the SysPatron will generate meaningless alarm information and record the problem in the log which affects the normal maintenance of the equipment.

4.6 Edit Registry Items of SysPatron?

Can the related setting of the SysPatron be configured in the registry?

It is recommended that you should not modify the related setting in the registry. Otherwise, the server cannot work normally or the SysPatron cannot be started.

4.7 Cannot Access Files or Use Applications After Installing SysPatron

After the installation of the SysPatron, double-click a program such as Windows Media Player, the computer always prompts “Access to the specified device, path, or file is denied”.

The cause is that the program is not added to the core file list. Open the configuration file ppt.log under the installation directory of the SysPatron, and check whether the program has been defined in the core file list [PROCESSES]. If not, the program must be added to the core file list.

4.8 SysPatron Still Functions After Uninstallation

Why does the SysPatron still function after it is uninstalled from the control panel?

It is not stopped before uninstalled. Although the registration information in the registry is deleted, the corresponding menu and service still exist. In this case, first use the operating control tool to stop its running, and reinstall the SysPatron. Then use the operating control tool to stop its running and uninstall it.

4.9 SysPatron Cannot Be Reinstalled After Uninstallation

It is possible that you have not uninstalled the SysPatron completely and the system monitoring function still works as described in question 7.

Solution: First stop the SysPatron (For details, refer to “3.3 Stopping the SysPatron”) and then reinstall it.

I. Whether can the log file be backed up to another computer automatically?

Reply: No.

At present, the log backup directory cannot be the disk of network mapping or network directory. Such backup directories as \\DataServer\LogDir are invalid.

II. Is the log directory invalid when the log backup directory is set to an invalid directory (such as j:\MyCD)?

Reply: No.

When the set log backup directory is invalid or null, the SysPatron copies the log file to be backed up to the subdirectory LogDir under the installation directory of the SysPatron automatically. If the subdirectory does not exist, it will be created automatically.

III. Does the SysPatron affect the installation and upgrade of the server software?

To install or upgrade the server software, first stop the running of the SysPatron. Because the installation program or upgrade program of the server software is not in the core file list of the SysPatron, you cannot execute it directly. After installing or upgrading the server software, you should upgrade the configuration file (especially the contents in the core file list) of the SysPatron based on the actual condition and generate verification files manually. Otherwise, the server software cannot work normally after the restart of the SysPatron. The frequently asked question is: After you reinstall or upgrade the server software, file version, patch and installation site are changed. However, the core file list is not modified accordingly so that the server software cannot be started.

IV. For the site that has installed and run the SysPatron, does the patch operation affect the server software?

The patch operation of the server software does not affect the running of the SysPatron. It is not necessary to generate verification files.

Generally, the operating system does not upgrade programs during the patch operation, so the patch operation does not affect the SysPatron. If the operating system upgrades programs during the patch operation, the SysPatron produces an alarm when you

restart the operating system. In this case, you just upgrade verification files based on specific alarm information.

V. Does the SysPatron protect against all the viruses?

The SysPatron cannot protect against all types of viruses. It only protects against those viruses that are spread through application programs.1

Appendix A Description of Installation Folders

By default, the installation directory of the system patron is C:\Program Files\huawei\SysPatron, in which programs and files are shown in Table A-1.

Table A-1 List of programs and files in the installation directory

Type	Name	Function
Core application file	SpyCenter.exe	System monitoring software, which monitors the startup of the WIN32 and to detect the integrity of programs and files on the server periodically.
Files	ppt.ini	Parameter configuration file, which is used to configure various working parameters of the system patron. For details, refer to “Appendix B Description of Configuration File”.
	WarnIn.dll	Alarm interface file, which defines the alarm structure.
	ppt.log	Log file, which records the running condition of the system patron.
	ProcActionSpy.sys	Driver of the system monitoring lower layer, which is a system file.
Support tools	SpyControl.exe	Operating control and integrity detection tool software, which starts and stops the system patron and helps you detect the integrity of programs and files.
	VerifyFileCreator.exe	Verification file generation tool, which verifies files or file lists and to generate verification files.

Appendix B Description of Configuration File

B.1 Editing Description of Configuration File

The configuration file of the system patron is ppt.ini. It is generated automatically under the installation directory when you install the system patron. This file is to configure various working parameters of the system patron. It affects the running condition of the system patron directly and be careful when you edit the file.

⚠ **Caution:**

Do not delete the file ppt.ini. Otherwise the system patron can not work normally.

The following should be noted when you modify the configuration file.

- Upon modifying the configuration of the file ppt.ini, the configuration is available. It is unnecessary to restart the system patron.
- There is no space between the segment name and the symbols "[" and "]". Otherwise the system cannot read configured parameters. For example, [BASIC] cannot be written as [BASIC].
- Do not edit or modify the names of the parameter segments ([BASIC], [PROCESSES], [FILES] and [WARNING]).
- The semicolon in the file indicates the subsequent content of the current line is remark information. The content following the semicolon is neglected during the information analysis. For example, “Basic parameter” in the “; Basic parameter” is the remark information.
- Based on descriptions in this manual, set parameter values correctly. For parameters out of the value range, the system patron replace them with default values automatically during the running of the system patron.
- You cannot use Chinese characters as punctuations in the file.
- When the system patron reads parameter values, it only reads the six bytes following the symbol “=”.

B.2 Description of Parameter Segments

B.2.1 Overview of Parameter Segments

The file ppt.ini includes the following parameter segments.

- Core file list parameter segment [PROCESSES]: It specifies important operating system programs or application programs that can be executed. These programs can run normally without real-time verification of process monitoring.
- Detection file list parameter segment [FILES]: It specifies important programs and files that require monitoring on the server. The detection file list and the core file list include verification files required in the system integrity detection.
- Timing detection parameter segment [BASIC]: It specifies related parameters about the system integrity timing detection, including the detection time and detection requirements.
- Log management parameter segment [BASIC]: It specifies related parameters about log management, including the maximum size and the maximum date saved of the log file.
- Alarm parameter segment [WARNING]: It specifies related parameters about alarms, including alarm type and alarm level.

B.2.2 Core File List [PROCESSES]

The core file list lists the important WIN32 programs on the server, including operating system programs and important application programs. Even through these files fail to generate verification files or errors occur in verification files, the process monitoring function of the system patron enables their running and produces the corresponding alarm prompt and log. If the important WIN32 programs are not added in the core list and fail to produce verification files for these files, these programs cannot be executed. Therefore, after installing the system patron, you must check parameter segments and supplement them based on the actual needs.

Note:

There are only two exceptions: the explorer program of Windows 2000 Server “Explorer.exe” and user initialization program “Userinit.exe”. These two programs are the important programs that must be executed when users log in the computer operating system. They are located respectively under the installation directory of Windows 2000 Server and the System32 subdirectory under the installation directory. No matter whether they have correct verification files or they are in the core file list, the system enables their running.

During the installation of the system patron, the installation program adds the full paths of important WIN32 (including directory names and file names where files are located) to the core file list. If the core file list is empty, the system patron produces alarm information and records the problem in the log.

The following is the automatically-generated core file list after the installation of the SoftX3000 system patron.

[PROCESSES]

C:\WINNT\system32\smss.exe

C:\WINNT\system32\csrss.exe

C:\WINNT\system32\winlogon.exe

C:\WINNT\system32\services.exe

C:\WINNT\system32\lsass.exe

C:\WINNT\system32\llssrv.exe

C:\WINNT\system32\userinit.exe

C:\WINNT\explorer.exe

C:\WINNT\system32\ntbackup.exe

C:\WINNT\system32\mmc.exe

C:\WINNT\system32\mshta.exe

C:\WINNT\system32\llsmgr.exe

C:\WINNT\system32\odbcad32.exe

C:\WINNT\system32\dllhost.exe

C:\WINNT\system32\cmd.exe

C:\WINNT\system32\svchost.exe

C:\WINNT\system32\taskmgr.exe

C:\WINNT\system32\shrpubw.exe

C:\WINNT\system32\rundll32.exe

C:\WINNT\system32\cleanmgr.exe

C:\WINNT\system32\msdtc.exe

C:\WINNT\system32\dfrgfat.exe

C:\WINNT\system32\dmadmin.exe

C:\WINNT\system32\sysocmgr.exe

C:\WINNT\system32\wbem\winmgmt.exe

C:\WINNT\system32\smlogsvc.exe

C:\WINNT\system32\netdde.exe

C:\WINNT\system32\mstask.exe

C:\WINNT\system32\attrib.exe

C:\WINNT\system32\eventvwr.exe

C:\WINNT\system32\mspaint.exe

C:\WINNT\system32\cliconfg.exe

C:\WINNT\system32\usrmgr.exe

C:\WINNT\system32\calc.exe

C:\WINNT\system32\drwtsn32.exe

C:\WINNT\system32\ntvdm.exe

C:\WINNT\system32\notepad.exe

C:\WINNT\notepad.exe

C:\Program Files\Windows NT\hypertrm.exe

C:\Program Files\Windows NT\dialer.exe

C:\Program Files\Windows NT\accessories\wordpad.exe

C:\WINNT\system32\systray.exe

C:\WINNT\system32\internat.exe

C:\WINNT\system32\conime.exe

C:\WINNT\hh.exe

C:\Program Files\Microsoft SQL Server\80\COM\distrib.exe

C:\Program Files\Microsoft SQL Server\80\COM\dw15.exe

C:\Program Files\Microsoft SQL Server\80\COM\logread.exe

C:\Program Files\Microsoft SQL Server\80\COM\qrdrsvc.exe

C:\Program Files\Microsoft SQL Server\80\COM\replmerg.exe

C:\Program Files\Microsoft SQL Server\80\COM\snapshot.exe

C:\Program Files\Microsoft SQL Server\80\COM\sqldumper.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\bcp.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\cdw.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\cnfgsvr.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\dcomscm.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\dtsrun.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\dtsrunui.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\dtswiz.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\isql.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\isqlw.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\itwiz.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\odbccmpt.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\osql.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\profiler.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\rebuildm.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\scm.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\sqladhlp.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\sqlftwiz.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\sqlmangr.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\svrnetcn.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\uncol.exe

C:\Program Files\Microsoft SQL Server\80\Tools\binn\wiztrace.exe

D:\SoftX3000\convert.exe

D:\SoftX3000\isuninst.exe

D:\SoftX3000\securitymanager.exe

D:\SoftX3000\uninstall.exe

D:\SoftX3000\wsgate.exe

D:\SoftX3000\services\bamservice.exe

D:\SoftX3000\services\bill.exe

D:\SoftX3000\services\billsorter.exe

D:\SoftX3000\services\dataman.exe

D:\SoftX3000\services\exchange.exe

D:\SoftX3000\services\isql.exe

D:\SoftX3000\services\logman.exe

D:\SoftX3000\services\maintain.exe

D:\SoftX3000\services\makecrc.exe

D:\SoftX3000\services\mml.exe

D:\SoftX3000\services\om_proc.exe

D:\SoftX3000\services\regsvr32.exe

D:\SoftX3000\services\smirror.exe

D:\SoftX3000\services\stats.exe

D:\SoftX3000\services\warn.exe

D:\SoftX3000\services\winsnmp_agent.exe

D:\SoftX3000\services\sntpclient.exe

D:\SoftX3000\bin\frame.exe

D:\SoftX3000\bin\mmlprn.exe

D:\SoftX3000\bin\regsvr32.exe

D:\SoftX3000\bin\stats.exe

D:\SoftX3000\bin\tracereview.exe

D:\SoftX3000\bin\warnws.exe

D:\SoftX3000\prttool\msgcl.exe

D:\SoftX3000\prttool\prescan.exe

D:\SoftX3000\prttool\prtgenerator.exe

D:\SoftX3000\tools\hwsetter.exe

D:\SoftX3000\tools\extablebrowser\extablebrowse.exe

D:\SoftX3000\tools\tablebrowser\tablebrowse.exe

C:\WINNT\smirror.exe

C:\WINNT\system32\perfmon.exe

C:\WINNT\system32\adjusttime.exe

C:\WINNT\system32\dynamicmonitor.exe

C:\WINNT\system32\virtualbam.exe

C:\Program Files\Microsoft SQL Server\MSSQL\BINN\SQLSERVR.EXE

C:\Program Files\Microsoft SQL Server\80\TOOLS\BINN\ISQLW.EXE

C:\Program Files\Microsoft SQL Server\80\TOOLS\BINN\ISQL.EXE

C:\Program Files\Microsoft SQL Server\80\TOOLS\BINN\SQLMANGR.EXE

Note:

- The programs under the directories C:\WINNT and C:\Program Files\Windows NT are the operating system programs.
- The programs under the directories C:\Program Files\Microsoft SQL Server are SQL database programs.
- The programs under the directories D:\SoftX3000 are the important application programs of the SoftX3000.

B.2.3 Detection File List [FILES]

The detection file list lists the important programs and data files on the server which are the objects of the system patron timing detection. This list cannot be generated automatically. Maintenance personnel should generate it manually.

When detecting the integrity of files, the system patron verifies programs and files in the detection file list and checks whether they have been modified or deleted. If these files are modified or deleted, the system patron generates an alarm and records the problem in the log.

The setting of the detection file list is same as that of the core file list. Both of them are written with the full paths of programs and files, as shown below:

[FILES]

D:\visio\Visio32.exe

D:\UltraEdit\UEDIT32.EXE

D:\office\Office10\WINWORD.EXE

……

B.2.4 Timing Detection Parameter [BASIC]

To prevent important programs or files from being modified or deleted, the system patron must verify those files periodically. If verification results are inconsistent with verification files, it indicates that programs or files have been modified or deleted. The system patron generates an alarm and records the problem in the log.

The parameter segment [BASIC] specifies the timing detection parameters. For specific parameter descriptions of the segment, see Table B-1 to Table B-5.

Table B-1 Parameter CHECKEACHDAY

Name	***CHECKEACHDAY***
Function	Determine whether to detect the integrity of the BAM system every day.
Value type	Character string
Value range	Any character string
Default value	If the parameter is set to “Y” or “y”, it indicates that the integrity is detected every day. If the parameter is set to any character string, it indicates that the integrity is detected every several hours.
Example	CHECKEACHDAY=Y indicates the integrity is detected every day.
Description	No semicolon following the parameter is used to add the remark information. Otherwise, the semicolon and the remark information will be regarded as one part of the character string.

Table B-2 Parameter INTERNAL

Name	***INTERVAL***
Function	Determine how often the integrity is detected. The parameter is valid only when the parameter "***CHECKEACHDAY***" is set to "Y" or "y".
Value type	Natural number. If the input number is not an integer, the decimal fraction is neglected automatically. If the input number is a negative, the minus sign is deleted automatically.
Value range	1–1193
Default value	For parameter values out of the value range, the default value is 12.
Example	INTERVAL=12 indicates the system integrity is detected every 12 hours.

Table B-3 Parameter CHECKTIME

Name	***CHECKTIME***
Function	Determine when the integrity is detected in a day. The parameter is valid only when the parameter "***CHECKEACHDAY***" is set to "Y" or "y".
Value type	Natural number. If the input number is not an integer, the decimal fraction is neglected automatically. If the input number is a negative, the minus sign is deleted automatically.
Value range	0–23
Default value	For parameter values out of the value range, the default value is 0.
Example	CHECKTIME =0 indicates the system integrity is detected at 12 midnight every day.

Table B-4 Parameter MAXSIZESUM

Name	***MAXSIZESUM***
Function	It defines the upper limit (Unit: M byte) of the size of the file to be detected. If the overall size of the file to be detected exceeds the upper limit, start the monitoring of CPU utilization. For details about the monitoring of CPU utilization, refer to Table B-5.
Value type	Natural number. If the input number is not an integer, the decimal fraction is neglected automatically. If the input number is a negative, the minus sign is deleted automatically.
Value range	10–1024
Default value	For parameter values out of the value range, the default value is 20.
Example	MAXSIZESUM=20 indicates the system checks CPU utilization when the file to be detected is larger than 20 M bytes.

Table B-5 Parameter BUSY

Name	***BUSY***
Function	Defines CPU utilization (percentage) when the system is busy. The parameter is valid only when the overall size of the file to be detected exceeds the set upper limit. When CPU utilization exceeds the parameter value, the system patron stops the timing detection. It continues when CPU utilization is less than the parameter value.
Value type	Natural number. If the input number is not an integer, the decimal fraction is neglected automatically. If the input number is a negative, the minus sign is deleted automatically.
Value range	1–100
Default value	For parameter values out of the value range, they are all set to 70..
Example	BUSY=70 indicates the system is busy when CPU utilization reaches 70%. In this case, the detection of the system patron is stopped.

B.2.5 Log Management Parameter [BASIC]

The log file ppt.log is stored under the installation directory of the system patron. The size of the log file increases with the running time of the system patron. If you do not back up the log file in time, you may lose the log due to the insufficiency of the disk space. Therefore, the system patron provides the backup function of the log file. It backs up the ppt.log under a specified directory. The name of the backup log file is the

original log file name + the date when the log is generated. Moreover, the system patron deletes log files saved for a long period periodically.

The parameter segment [BASIC] specifies log management parameters. For specific parameter descriptions of the segment, see Table B-6 to Table B-8.

Table B-6 Parameter MAXLOG

Name	***MAXLOG***
Function	Define the maximum byte number of ppt.log (Unit: M byte).
Value type	Natural number. If the input number is not an integer, the decimal fraction is neglected automatically. If the input number is a negative, the minus sign is deleted automatically.
Value range	1–20
Default value	For parameter values out of the value range, the default value is 5.
Example	MAXLOG=5 indicates the maximum byte number of ppt.log is 5 M.

Table B-7 Parameter LOGPERIOD

Name	***LOGPERIOD***
Function	Define the maximum date saved of the backup log file
Value type	Natural number. If the input number is not an integer, the decimal fraction is neglected automatically. If the input number is a negative, the minus sign is deleted automatically.
Value range	1–365
Default value	For parameter values out of the value range, the default value is 30.
Example	LOGPERIOD=30 indicates the backup log file can be saved for 30 days at most.

Table B-8 Parameter BACKUPLOGDIR

Name	***BACKUPLOGDIR***
Function	It specifies the directory that saves the backup log file.
Value type	Character string.
Value range	Valid directory name, which cannot be the disk of the network mapping or network directory, such as \\DataServer\LogDir. If the set backup directory does not exist, the system creates the directory automatically.
Default value	If the parameter is set to empty, the system backs up the log file under the subdirectory LogDir of the installation directory.
Example	BACKUPLOGDIR= indicates the backup directory of the log file is set to empty. The automatic backup log file is stored under the subdirectory LogDir of the installation directory.

B.2.6 Alarm Parameter [WARNING]

The alarm interface file Warnln.dll specifies the structure of alarm message in the system patron. The parameter segment [WARNING] of the file ppt.ini specifies the value range of various fields in the structure.

HUAWEI

U-SYS SoftX3000 SoftSwitch System
BAM User Manual

Part 2 iWeb Remote Maintenance Access System

Table of Contents

Chapter 1 System Description 1-1
1.1 Overview of iWeb Maintenance Access System 1-1
1.2 Service Models 1-1
1.2.1 Overview of Service Models 1-1
1.2.2 Typical Configurations 1-1
1.2.3 Configuration Guidelines 1-5
1.2.4 Remote Access Server RAS 1-7
1.2.5 Remote Access Client RAC 1-8
1.3 System Functions of iWeb system 1-10
1.3.1 Access Control of iWeb system:access control 1-10
1.3.2 Connection Management of iWeb system:connection management 1-10
1.3.3 Two-Way Data Transmission of iWeb system:two-way data transmission 1-10
1.3.4 Data Compression and Encryption of iWeb system:data compression and encryption 1-11
1.3.5 Traversing Firewalls and Proxy Servers of iWeb system:traversing firewalls and proxy servers 1-11
1.4 Technical Features of iWeb system 1-11
1.4.1 Little System Structure Change 1-11
1.4.2 Configurable Access Control Strategy 1-12
1.4.3 Compression and Encryption Based on Ports 1-12
1.4.4 Adjusted Network Bandwidth 1-12
1.4.5 Automatic Retry Connection 1-12
1.4.6 Support from Multiple Maintenance Terminals 1-12
1.5 Software and Hardware Configuration 1-12
1.5.1 Hardware Configuration 1-12
1.5.2 Software Configuration 1-13

Chapter 2 Software Installing and Uninstalling 2-1
2.1 Software Installation 2-1
2.1.1 Installation Flow 2-1
2.1.2 Installation Preparations 2-2
2.1.3 Installing JDK Software 2-3
2.1.4 Installing RAS Software 2-8
2.1.5 Check for RAS Software Installation 2-14
2.1.6 Installing RAC Software 2-16
2.1.7 Check for RAC Software Installation 2-16
2.2 Uninstalling Software 2-17
2.3 Frequently Asked Question in Software Uninstallation 2-20

Chapter 3 Operation Guide 3-1
3.1 Overview of Operation Guide 3-1
3.2 Introduction to Service Interfaces 3-1
3.2.1 RAS Service Interface 3-1
3.2.2 RAC Service Interface 3-3
3.3 RAS Data Configuration 3-4
3.3.1 Configuring IP Address and Ports 3-5
3.3.2 Configuring Multi-Language Attribute 3-6
3.3.3 Configuring Log Functions 3-8
3.3.4 Configuring Connection Instances 3-9
3.3.5 Configuring Server Types 3-16
3.3.6 Configuring Server Instances 3-20
3.4 RAC Data Configuration 3-24
3.4.1 Configuring the System Attribute File 3-24
3.4.2 Configuring Log Functions 3-25
3.4.3 Configuring Proxy Information 3-25
3.4.4 Configuring Maintenance Terminal Access Strategy 3-27
3.5 RAS Basic Operation 3-30
3.5.1 Starting RAS Background Service 3-30
3.5.2 Logging in RAS Service Interface 3-31
3.5.3 Reviewing Connection Requests Manually 3-31
3.5.4 Changing RAS Login Password 3-33
3.5.5 Logging Out RAS 3-35
3.5.6 Showing Online Help 3-36
3.5.7 Closing RAS Background Service 3-38
3.6 RAC Basic Operation 3-38
3.6.1 Logging in RAC Service Interface 3-38
3.6.2 Changing RAC Login Password 3-38
3.6.3 Locking and Unlocking 3-39
3.6.4 Establishing/ Deleting a Connection to RAS 3-39
3.6.5 Activating/Deactivating a Connection to RAS 3-45
3.6.6 Manual-Refresh/Auto-Refresh Connection Status 3-46
3.6.7 Changing RAC Interface Display Mode 3-47
3.6.8 Showing Online Help 3-48
3.6.9 Showing the iWeb System Version Information 3-48
3.6.10 Logging Out RAC 3-49
3.6.11 Exiting RAC Service Interface 3-49
3.7 A Typical Maintenance Example 3-50
3.7.1 Description of Example 3-50
3.7.2 Configuring RAS Data 3-50
3.7.3 Configuring the RAC Data 3-50
3.7.4 Creating Connection from RAC to RAS 3-51

3.7.5 Starting Remote Maintenance 3-51
3.7.6 Ending Remote Maintenance 3-51
3.8 FAQ on Remote Maintenance 3-51
3.8.1 One RAC Cannot Activate Multiple Maintenance Terminals? 3-51
3.8.2 RAC Cannot Refresh Connection Status or Start Connection? 3-52
3.8.3 Maintenance Terminal Cannot Receive Response from Server in Time? 3-52
Appendix A Description of RAS Installation Directory A-1
Appendix B Description of RAC Installation Directory B-1

Chapter 1 System Description

1.1 Overview of iWeb Maintenance Access System

With the increasing development of the telecom market, more areas are covered by telecommunication equipment, and requirements for remote maintenance of equipment are stricter. At present, the frequently-used remote maintenance is to access remote servers in the dial-up mode. It features low configuration requirement and easy operation. However, it has slow communication speed, poor reliability and expensive cost.

Therefore, Huawei developed the iWeb remote maintenance access system. The Internet-based system adopts the server/client architecture. It connects a maintenance terminal with a remote server through an access server and an access client. It implements the two-way data transmission between a maintenance terminal and a remote server through Hyper Text Transport Protocol (HTTP) and Hyper Text Transport Protocol Secure (HTTPS) for remote maintenance. Compared with the dial-up access mode, the iWeb remote maintenance access system features fast communication speed, high reliability, and low maintenance cost.

1.2 Service Models

1.2.1 Overview of Service Models

The iWeb remote maintenance access system is to provide rapid and safe two-way data channel for remote maintenance. It has many configuring modes to meet different requirements for application.

1.2.2 Typical Configurations

I. Basic Configuration

The iWeb remote maintenance access system consists of the remote access server (RAS) and the remote access client (RAC). The basic configuration is shown in Figure 1-1.

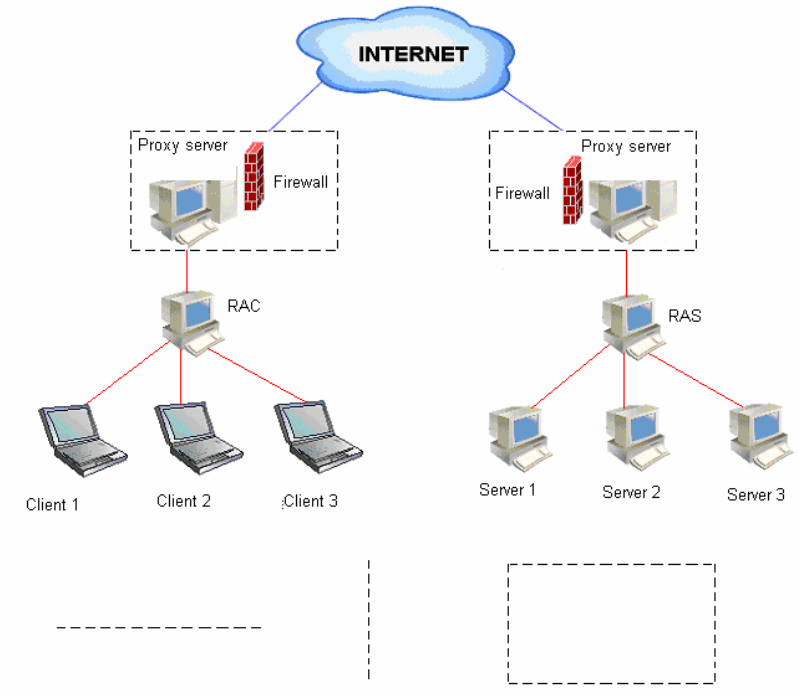


Figure 1-1 Basic configuration

In the above figure, the maintenance terminals and the RACs are in the same subnet. The servers and the RASs are in another subnet. The above subnets access Internet through proxy servers. Maintenance terminals access servers through RACs, RASs, and proxy servers.

II. Features of Basic Configuration

- Proxy servers can access multiple RACs or RASs.

By separating RACs from maintenance terminals and separating RASs from servers, they can manage RACs and RASs in a centralized mode, increasing the security of the access system and avoiding the effect of server upgrading on the system.

- The equipment cost increases.

Because the RAC and the RAS use dedicated servers

Need human intervention on the maintenance terminals and the RAC.

Notes:

The RAC (RAS) must provide maintenance ports. Otherwise, it cannot connect with maintenance terminals (servers) to implement maintenance function. Moreover, the RAC and the RAS must provide HTTP and HTTPS ports to interconnect with each other through proxy servers.

In addition to the basic configuration, you can combine some parts to establish other configuration modes based on actual needs. The following introduces some frequently-used configuration modes.

III. Combination Between RAC and Maintenance Terminals, RAS and Proxy Servers

The system networking is shown in Figure 1-2. The strong points of the configuration are: The equipment cost decreases because the RAC and the RAS do not use a separate server, and maintenance operation focuses on maintenance terminals. Thus, it is convenient for operation. The weak points are: Proxy servers must provide maintenance ports to connect with servers, which are restricted by firewalls, so the firewall setting must be modified. Moreover, RACs combine with maintenance terminals so that it is difficult to manage them and the system security is affected.

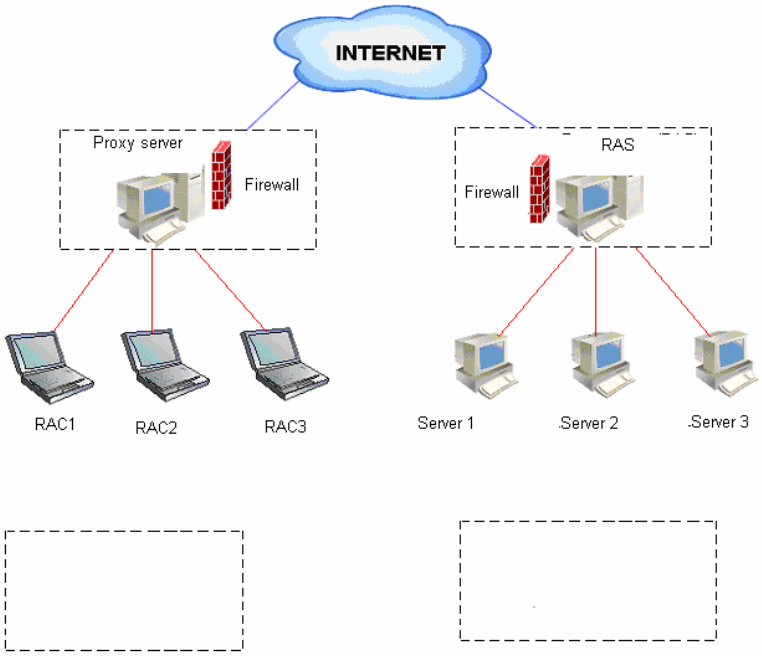


Figure 1-2 Typical configuration model 1

IV. Combination Between RAS and Server

The system networking is shown in Figure 1-3. The configuration realizes the centralized management similar to that of the RAC and the RAS in the basic configuration. The RAS does not use a special server, so the cost is decreased. However, maintenance operation is still inconvenient. After combination of the RAS and a server, the access system is likely to be affected by server upgrading.

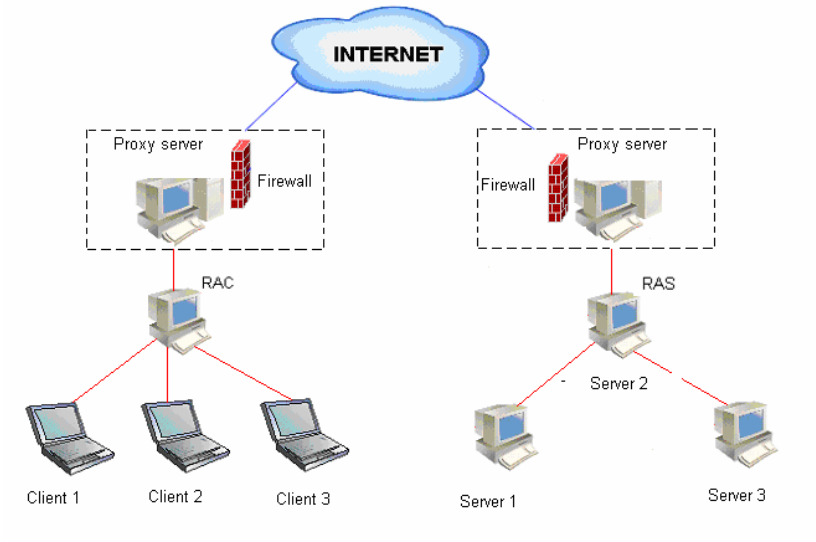


Figure 1-3 Typical configuration model 2

V. Direct Access to Internet by RAC

The system networking is shown in Figure 1-4. The configuration does not need a proxy server on the maintenance terminal side. The structure is simple. However, maintenance terminals are vulnerable to illegal attacks because they access Internet directly. Similar to the previous configuration, the access system can be affected easily during server upgrading. The configuration is applicable to the following two conditions:

- A proxy server is faulty.
- Maintenance engineers log onto the Internet in the dial-up or broadband mode to maintain equipments in distance. The RAC and a maintenance terminal can be combined on the same computer to facilitate maintenance operation.

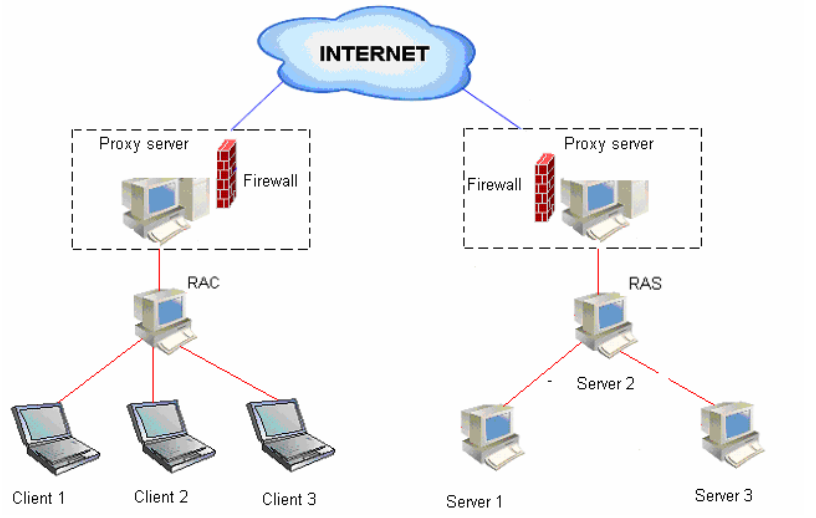


Figure 1-4 Typical configuration model 3

1.2.3 Configuration Guidelines

The following takes the basic configuration as an example to describe the operating principle of the iWeb remote maintenance access system. In Figure 1-1, suppose you plan to remotely maintain the server 3 through maintenance terminal 1. Figure 1-5 shows the basic operation procedure.

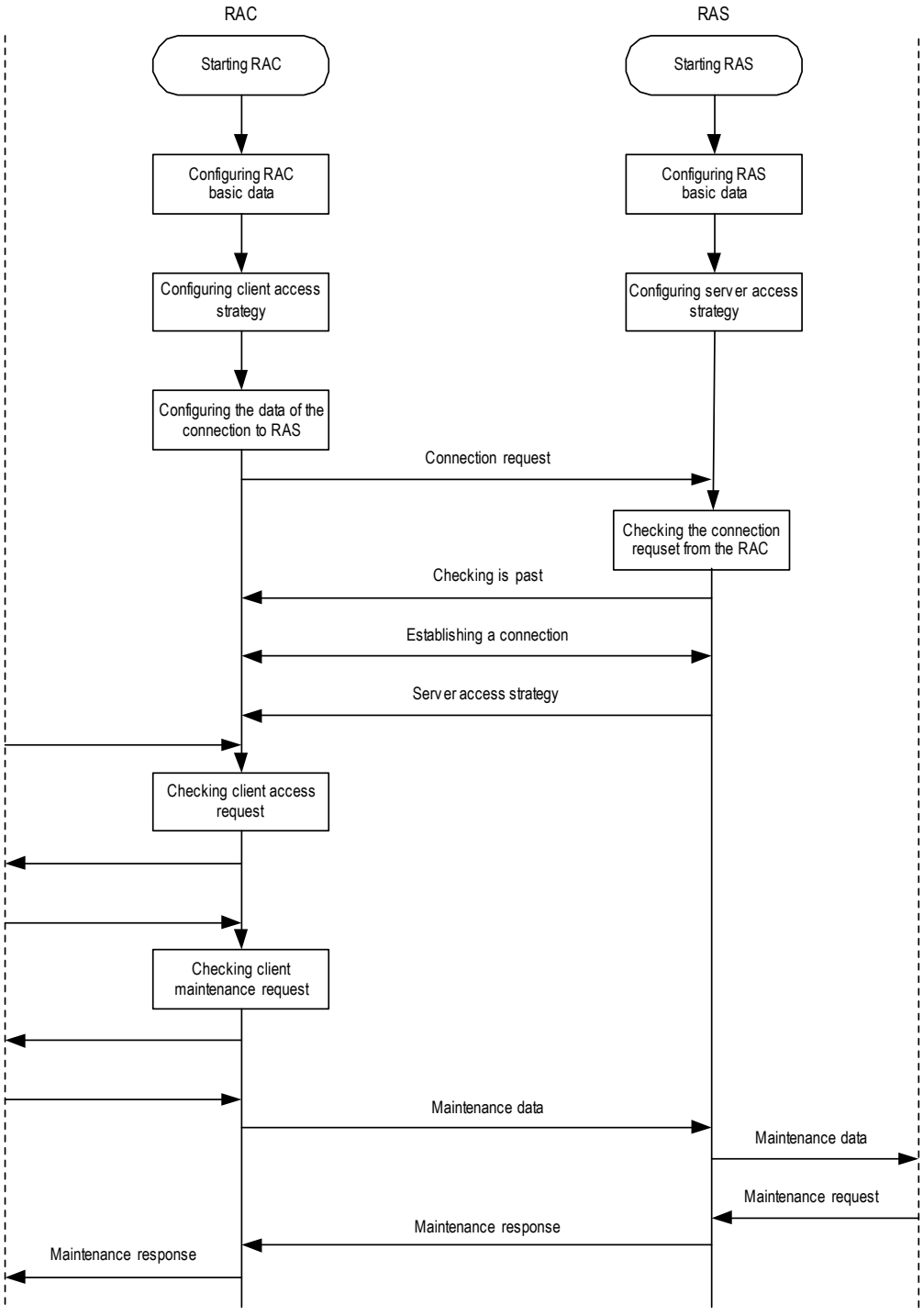


Figure 1-5 Operating principle of the iWeb remote maintenance access system

1) The RAS administrator configures basic data on the RAS, including IP address, ports, multi-language attribute, and log functions of the RAS.
2) The RAS administrator configures server access strategy on the RAS (that is, the administrator determines which servers can be maintained remotely), and pre-configures some connection examples at the same time. In this example, server 3 can be set to be maintained remotely.
3) The RAC administrator configures basic data on RAC, including language, country attribute, log functions and proxy data of the RAC.
4) The RAC administrator configures maintenance terminal access strategy on the RAC; that is, the administrator determines which maintenance terminals can access the RAC. In this example, maintenance terminal 1 can be set to access the RAC.
5) The RAC administrator configures data for connections between RAC and RAC on the RAC, including IP address and channel of the RAS, and activates the configuration to send a connection request to the RAS.
6) On receiving the connection request, the RAS administrator authenticates it. If the corresponding connection has been configured, the connection request passes the authentication automatically. Otherwise, the request must be authenticated manually on the RAS. The connection can be established only when the connection request passes the authentication.
7) After successful authentication, the RAS establishes a connection with the RAC and sends the configured server access strategy to the RAC.
8) Maintenance terminal 1 connects with the RAC. The RAC approves or refuses the connection request based on maintenance terminal access strategy.
9) When maintenance terminal 1 connects with the RAC successfully, it sends a remote maintenance request for server 3.
10) The RAC checks the remote maintenance request based on server access strategy. If the target server in maintenance requirements has been configured in the server access strategy, the authentication is successful and the operator can carry out maintenance operations on the maintenance terminal. Otherwise, maintenance operation fails. Because server 3 is configured in server access strategy in this example, the authentication succeeds, and you can operate maintenance at maintenance terminal 1.
11) The RAC begins to receive maintenance data from maintenance terminal 1 and then transfers it to the RAS in a packet.
12) On receiving the maintenance data, the RAS restores data through disassembly. The RAS transmits the maintenance data to server 3, and then sends the response from server 3 to maintenance terminal 1 through the RAC.

Note:

The RAC and the RAS are connected through HTTP and HTTPS to traverse firewalls and proxy servers.

The connection between RAC and RAS is broken if either of them deactivates or disconnects it.

1.2.4 Remote Access Server RAS

I. Overview of RAS

As a proxy of the server, the RAS receives and transmits maintenance data and response data. Besides, such measures as authentication of connection requests and connection time limit are taken to ensure the security and reliability of remote maintenance operation.

The RAS has the following functions:

II. System Management

The system management means management and maintenance for RAS itself, including:

- Adding/deleting an RAS user and password;
- Starting/stopping an RAS;
- Logging in/logging out the RAS;
- Changing the RAS user password.

III. Connection Management

Connection management means management and maintenance for the connection between RAS and RAC, including:

- Authenticating connection requests from the RAC;
- Adding connections;
- Refreshing connections;
- Deleting connections;
- Setting related connection attributes (such as automatic disconnection time).

IV. Equipment Server Access Strategy Management

Equipment server access strategy management means which servers attached to the RAS can be maintained remotely. Equipment server access strategy management includes:

- Adding/deleting server types; that is, setting which types of servers can be maintained. When the RAC checks maintenance requests from maintenance terminals, the configuration data can be used.

- Adding/deleting server instances; that is, designating maintainable servers. When the RAC checks maintenance requests from maintenance terminals, this configuration data can be used.

V. Data Management

Data management means the RAS receives maintenance data from the RAC and transmits it to the corresponding server after disassembly. Meanwhile, the RAS receives responses from servers and then transmits them to the RAC after packet assembly.

Note:

If you plan to compress and encrypt data during the transmission, compress and encrypt it after assembly, and decompress and decrypt it after disassembly.

1.2.5 Remote Access Client RAC

I. Overview of RAC

As a proxy of the maintenance terminal, the RAC checks maintenance requests from maintenance terminals. After the check, the RAC begins to collect and transmit maintenance data from maintenance terminals, and receive responses from the RAS and transmit it to the corresponding maintenance terminals.

The RAC has the following functions:

- System management
- Connection management
- Access strategy management
- Maintenance management
- Data management

II. System Management

The system management means management and maintenance for the RAC itself, including:

- Adding/deleting an RAC user and password;
- Starting/stopping an RAC;
- Logging in/logging out an RAC;
- Changing the RAC user password;
- Setting an RAC general option;
- Setting an RAC security option.

III. Connection Management

Connection management means management and maintenance for connections between RAS and RAC, including:

- Establishing connections;
- Deleting connections;
- Checking connection attributes;
- Activating connections;
- Deactivating connections;
- Refreshing connections manually;
- Refreshing connections automatically.

IV. Access Strategy Management

Maintenance terminal access strategy management is to define which maintenance terminal can be connected to the RAC to carry out the maintenance operation. It includes:

- Adding IP addresses of maintenance terminals that can access the RAC.
- Deleting IP addresses of maintenance terminals that cannot access the RAC.

V. Maintenance Management

Maintenance management means the RAC checks maintenance requests from maintenance terminals based on the server access strategy from the RAS. If destination servers in maintenance requests have been configured in the server access strategy; that is, destination servers can be maintained remotely, the RAC begins to transmit maintenance data. Otherwise, the RAC will refuse maintenance requests.

VI. Data Management

Data management means the RAC receives maintenance data from maintenance terminals and sends it to the RAS after assembly, and receives server response data from the RAS and transmits it to the corresponding maintenance terminals after disassembly.

Note:

If you plan to compress and encrypt data during the transmission, you need to compress and encrypt data after assembly, and decompress and decrypt after disassembly.

1.3 System Functions of iWeb system

The iWeb remote maintenance access system provides a secure and efficient communication channel for maintenance terminals and servers. It includes the following functions.

1.3.1 Access Control of iWeb system:access control

Access control means communication channels are established between maintenance terminals and equipments based on the server access strategy and the maintenance termianal access strategy. It includes the following parts:

I. Access Control on the RAS Side

As described in “1.1.3 Remote Access Server RAS”, the RAS authenticates connection requests from an RAS by configuring the “Client Session List” based on the server access strategy. The list includes all connecting information from the authenticated RAC to the server.

II. Access Control on the RAC Side

As described in “1.1.4 Remote Access Client RAC”, the RAC checks maintenance requests from maintenance terminals to ensure the validity of maintenance operation based on the server access strategy from the RAS. Meanwhile, the RAC checks connection requests from maintenance terminals to ensure the security of the system based on the maintenance terminal access strategy.

III. Security Management of Access System

Both RAS and RAC provide user login function to ensure the security of the access system.

1.3.2 Connection Management of iWeb system:connection management

The RAS controls the access of the RAC through connection management and ensures the access security and reliability by setting connection automatic disconnection time. Moreover, the RAC can maintain the connection. For details, refer to "Connection Management" in “1.1.3 Remote Access Server RAS” and “1.1.4 Remote Access Client RAC”.

1.3.3 Two-Way Data Transmission of iWeb system:two-way data transmission

The RAS and the RAC combine to implement two-way data transmission between maintenance terminals and servers. For details, refer to "Connection Management" in “1.1.3 Remote Access Server RAS” and “1.1.4 Remote Access Client RAC”.

1.3.4 Data Compression and Encryption of iWeb system:data compression and encryption

In the iWeb remote maintenance access system, compression and encryption technology of port level can be used to transmit data between RAC and RAS. Data compression can increase the rate of data transmission, implement efficient bandwidth usage, and adapt to low-bandwidth access (such as dial-up access). Data encryption can increase the security of data transmission.

Note:

Both compression and encryption are optional. You can determine whether to use them based on actual needs.

1.3.5 Traversing Firewalls and Proxy Servers of iWeb system:traversing firewalls and proxy servers

To prevent virus infection and illegal attack, proxy servers and firewalls are installed between telecom equipments and Internet. If a maintenance terminal and a server are not in the same network segment, and a proxy server does not support remote maintenance protocol or a firewall disables maintenance ports, the maintenance terminal cannot carry out remote maintenance. This is what must be solved for the remote maintenance access system.

Data can be transmitted between RAS and RAC through HTTP and HTTPS. That is what The iWeb remote maintenance access system has solved properly. At present, proxy servers support HTTP and HTTPS and most firewalls open HTTP ports.

1.4 Technical Features of iWeb system

Compared with other remote maintenance access systems, the iWeb remote maintenance access system has the following features:

1.4.1 Little System Structure Change

The iWeb remote maintenance access system only requires that the RAC and the RAS are added to the current system. Therefore, the system structure is changed little. If you combine the RAS and a proxy server, and combine the RAC and a maintenance terminal, the system structure is almost not changed.

1.4.2 Configurable Access Control Strategy

By configuring server access strategy and maintenance terminal access strategy, the IWeb remote maintenance access system can control remote maintenance effectively. Only maintenance terminals that meet the requirements of the maintenance terminal access strategy can connect with the RAC to maintain servers which must be defined in the server access strategy.

1.4.3 Compression and Encryption Based on Ports

Data compression and encryption of port level means the compression and encryption for the data transmitted on specific ports. Compared with other compression and encryption technologies, data compression and encryption of port level can operate lower layer data directly with fast operating speed and good security.

1.4.4 Adjusted Network Bandwidth

When connecting RAC with RAS, you can adjust bandwidth attributes of the connecting port depending on actual requirements. You can obtain higher response speed by increasing bandwidth of the port, or save network resources by decreasing bandwidth of the port.

1.4.5 Automatic Retry Connection

If the RAC fails to connect with the RAS, it can try to connect the RAS automatically based on the predefined retry strategy (including retry times and designated time interval)

1.4.6 Support from Multiple Maintenance Terminals

One RAC can access multiple maintenance terminals simultaneously, but only one maintenance terminal can be activated at any time. That is to say, you can just operate remote maintenance on one of the maintenance terminals. One RAS can be connected with multiple RACs. You can remotely maintain multiple servers under different RASs on one maintenance terminal, but you can just remotely maintain one server under any RAS at any time.

1.5 Software and Hardware Configuration

1.5.1 Hardware Configuration

Specific hardware configuration requirements of the RAS and the RAC are listed in Table 1-1 and Table 1-2.

Table 1-1 RAS hardware configuration requirements

Configuration item	Minimum system requirement
Host	PC (It can combine with the current server.)
CPU	886 MHz
RAM	128 MB

Table 1-2 RAC hardware configuration requirements

Configuration item	Minimum system requirement
Host	Desktop or portable PC (It can combine with the current maintenance terminal.)
CPU	886 MHz
RAM	128 MB

1.5.2 Software Configuration

I. Software Composition of the iWeb Remote Maintenance Access System

Software of the iWeb remote maintenance access system consists of the RAS software and the RAC software. For the specific software composition, refer to “Appendix A Description of RAS Installation Directory” and “Appendix B Description of RAC Installation Directory”.

II. Matched Software

Configuration requirements of matched software of the RAS and the RAC are listed in Table 1-3 and Table 1-4

Table 1-3 RAS matched software requirements

Type	Name and version
Operating system	Microsoft Windows NT, Microsoft Windows XP, Microsoft Windows 2000
Browser	Internet Explorer 5.5 or later
JDK	JDK 1.3.1.07 (It provides the JAVA environment required in the RAS running.)

Table 1-4 RAC matched software requirements

Type	Name and version
Operating system	Microsoft Windows NT, Microsoft Windows XP, Microsoft Windows 2000
Browser	Internet Explorer 5.5 or later
JRE/JDK	JRE 1.3.1.07/JDK 1.3.1.07 (It provides the JAVA environment required in the RAC running. You can install one of them. This manual only introduces the installation of the JDK softaware.)

Chapter 2 Software Installing and Uninstalling

2.1 Software Installation

2.1.1 Installation Flow

Software installation of the iWeb remote maintenance access system includes the following two parts:

- Access server software installation
- Access client software installation

The installation flows are as shown in Figure 2-1 and Figure 2-2 respectively. This chapter only introduces the installation of the JDK software, the RAS software, and the RAC software. It does not cover the installation of an operating system and a browser. To install an operating system and a browser, refer to the corresponding technical materials or follow the setup wizard prompt.

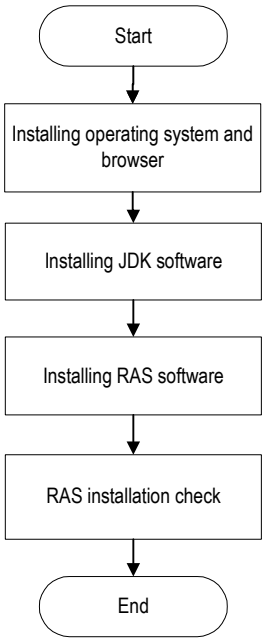


Figure 2-1 Installation flow of access server software

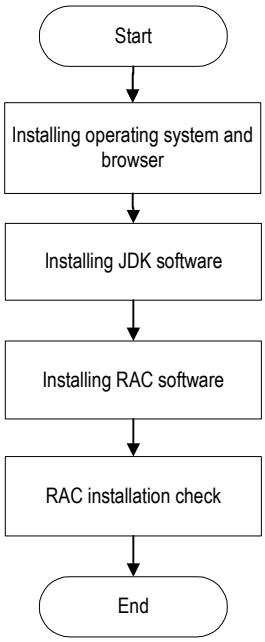


Figure 2-2 Installation flow of access client software

2.1.2 Installation Preparations

I. Preparations for RAS Installation

First, a computer to be installed with the RAS software must be in the same subnet with servers. In addition, the subnet is connected with the Internet; that is, maintenance terminals can access the RAS through the Internet. Next, the computer installed with the RAS software must meet the hardware configuration requirements in Table 1-1.

II. Preparations for RAC Installation

The RAC can be combined either with a special-purpose computer or with a maintenance terminal directly. It is recommended to install the RAC on a maintenance terminal directly to facilitate remote maintenance operation and reduce equipment investment. The subnet where the RAC is located must be connected with the Internet; that is, the RAC can access to servers through the Internet. The computer installed with the RAC software must meet the hardware configuration requirements in Table 1-2.

III. Preparations for Software Installation

In addition to preparations for software installation programs of the RAS and the RAC, you need to prepare the matched software installation programs, which are listed in Table 1-3 and Table 1-4.

2.1.3 Installing JDK Software

Before installing the RAS software and the RAC software, you must install the JDK software. Otherwise, the RAS software and the RAC software cannot run normally. Moreover, after installing the JDK software, you must configure corresponding environment variables to enable the JDK software. Taking access server as an example, the following shows the JDK software installation:

Note:

Installing the JDK software on the access client is the same as installing that on the access server. You can refer to this section for corresponding installation of JDK software on the access client.

I. Installing JDK Software

1) Put the installation disk of the iWeb remote maintenance access system in CD-ROM. Double click the installation program j2sdk-1_3_1-win.exe to install the JDK.
2) The window "Welcome" is displayed, as shown in Figure 2-3. Click <Next>.

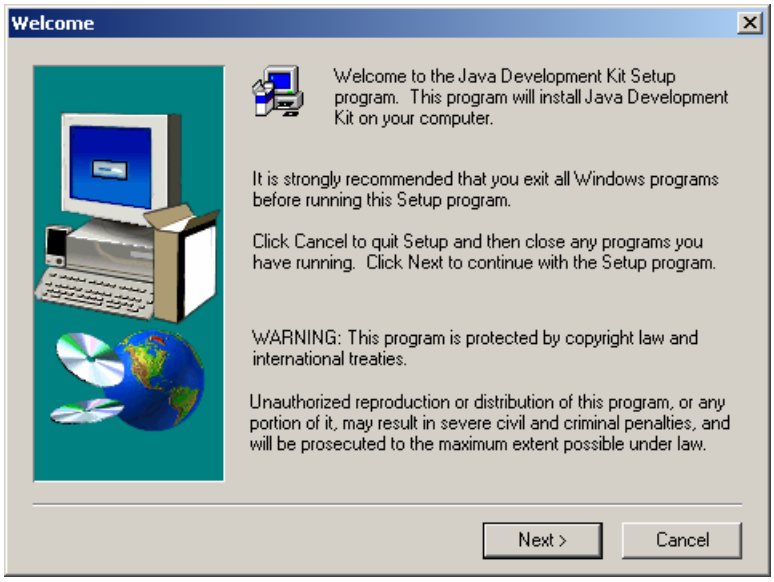

Welcome
Welcome to the Java Development Kit Setup program. This program will install Java Development Kit on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel

Figure 2-3 “Welcome” window

3) The window “Software License Agreement” is displayed, as shown in Figure 2-4. Click <Yes> if you accept this agreement.

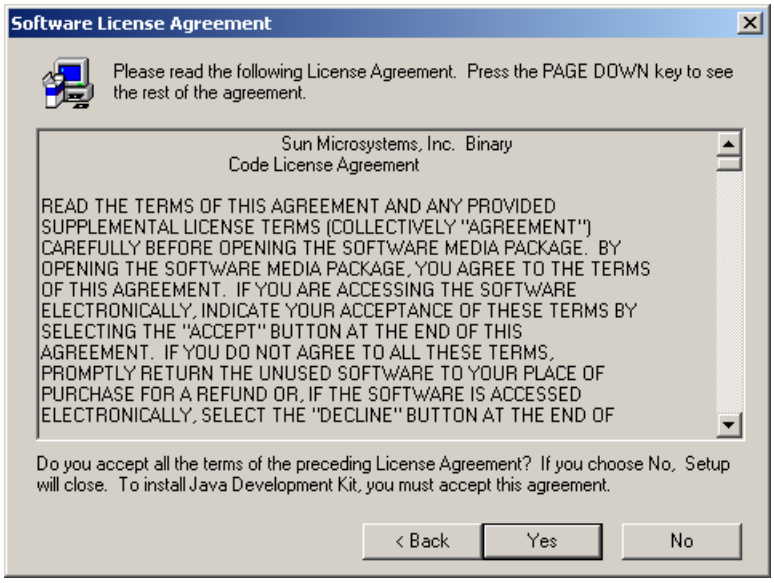

Software License Agreement
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.
Sun Microsystems, Inc. Binary Code License Agreement
READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE OPENING THE SOFTWARE MEDIA PACKAGE. BY OPENING THE SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install Java Development Kit, you must accept this agreement.
< Back
Yes
No

Figure 2-4 “Software License Agreement” window

4) The window “Choose Destination Location” is displayed, as shown in Figure 2-5 . Click <Browse> to select an installation directory. It is recommended to select the default installation directory C:\jdk1.3.1. Click <Next> after choosing an installation directory.

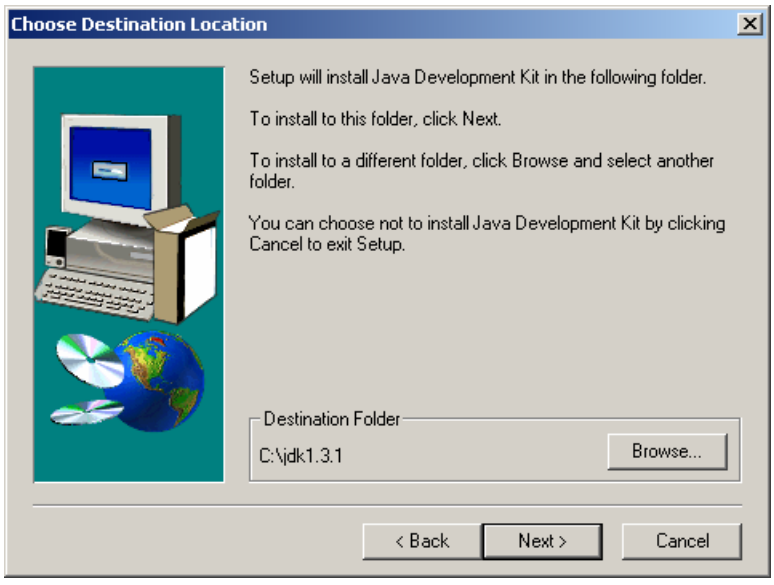

Choose Destination Location
Setup will install Java Development Kit in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install Java Development Kit by clicking Cancel to exit Setup.
Destination Folder
C:\jdk1.3.1
Browse...
< Back
Next >
Cancel

Figure 2-5 “Choose Destination Location” window

5) The window “Select Components” is displayed, as shown in Figure 2-6. All the installation components are selected by default. Click <Next>.

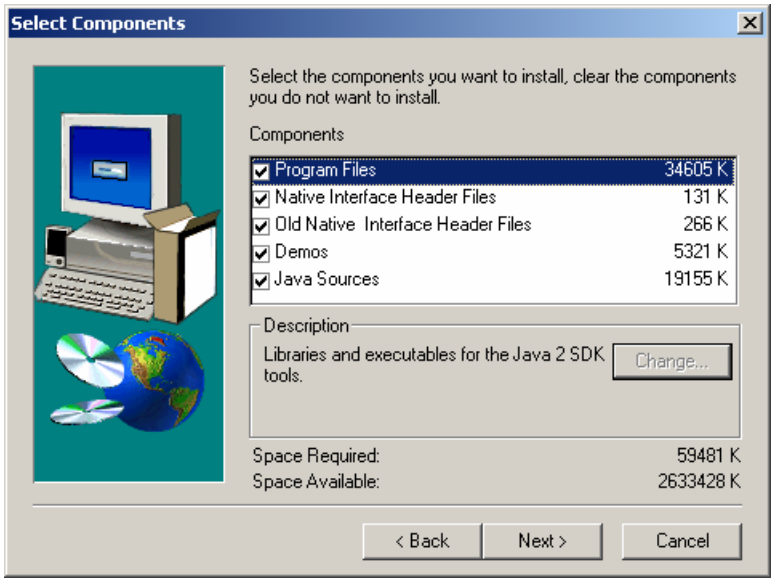

Select Components
Select the components you want to install, clear the components you do not want to install.
Components
Program Files 34605 K
Native Interface Header Files 131 K
Old Native Interface Header Files 266 K
Demos 5321 K
Java Sources 19155 K
Description
Libraries and executables for the Java 2 SDK tools.
Change...
Space Required: 59481 K
Space Available: 2633428 K
< Back
Next >
Cancel

Figure 2-6 "Select Components" window

6) After all the files are copied to the computer, the window "Setup Complete" is displayed, as shown in Figure 2-7.

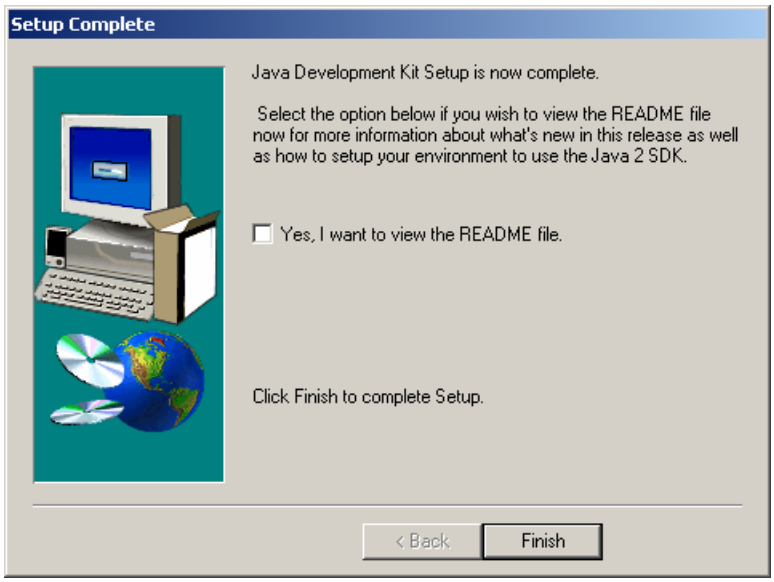

Setup Complete
Java Development Kit Setup is now complete.
Select the option below if you wish to view the README file now for more information about what's new in this release as well as how to setup your environment to use the Java 2 SDK.
Yes, I want to view the README file.
Click Finish to complete Setup.
< Back
Finish

Figure 2-7 "Setup Complete" window

Click <Finish>.

II. Setting Environment Variables

1) On the desktop, select the "My Computer" icon. Right click and select <Properties> in the shortcut menu.
2) The window "System Properties" is displayed. Select the tab "Advanced", as shown in Figure 2-8.

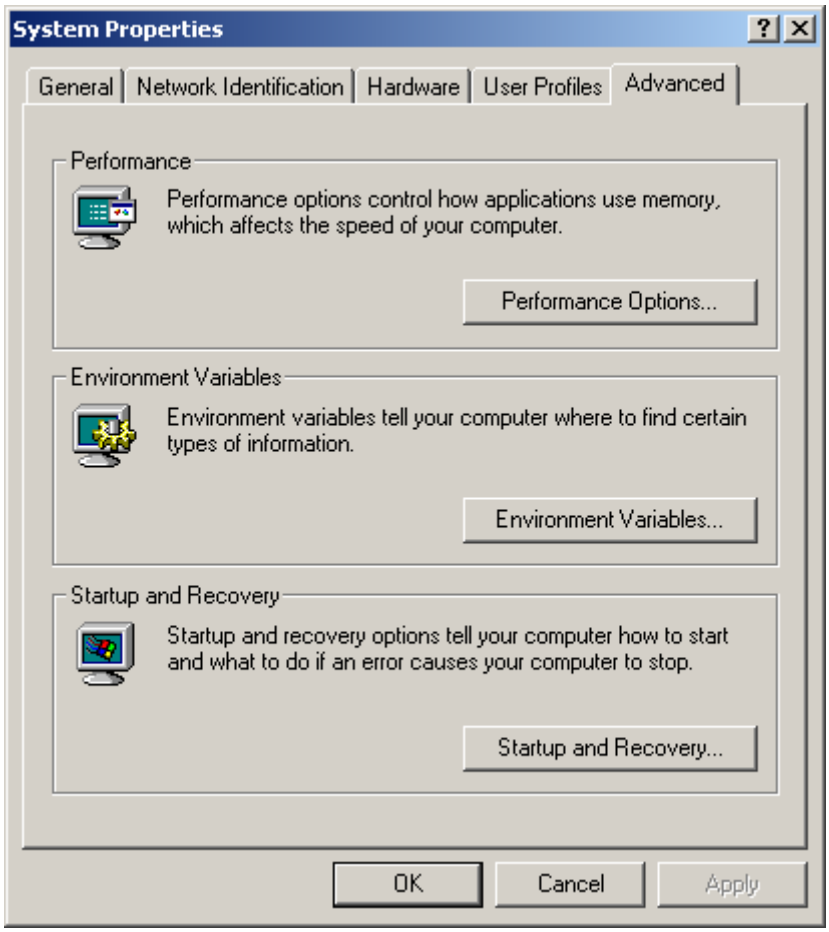

System Properties
General
Network Identification
Hardware
User Profiles
Advanced
Performance
Performance options control how applications use memory, which affects the speed of your computer.
Performance Options...
Environment Variables
Environment variables tell your computer where to find certain types of information.
Environment Variables...
Startup and Recovery
Startup and recovery options tell your computer how to start and what to do if an error causes your computer to stop.
Startup and Recovery...
OK
Cancel
Apply

Figure 2-8 “System Properties” window

3) Click <Environment Variables> in Figure 2-8. Then the window “Environment Variables” is displayed, as shown in Figure 2-9.

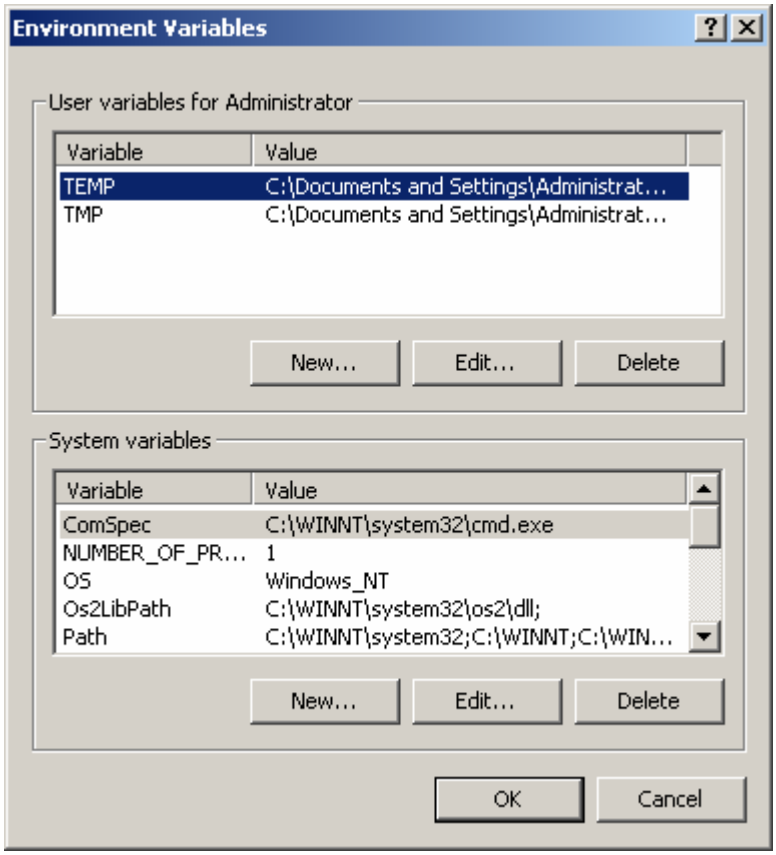


Figure 2-9 “Environment Variables” window

4) Click <New> under the window “System variables” in Figure 2-9. Then the dialogue box "New System Variable" is displayed, as shown in Figure 2-10. Enter JAVA_HOME in the “Variable Name” box, and enter the default installation directory C:\jdk1.3.1 in the “Variable Value” box. Click <OK>

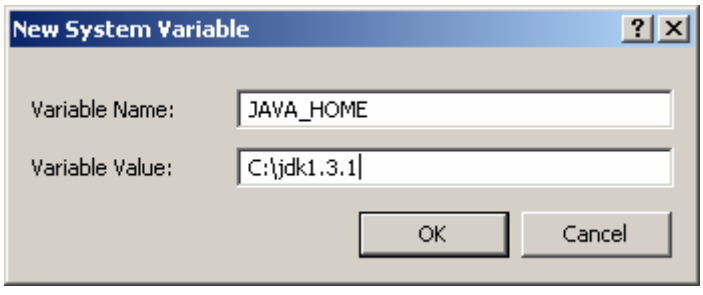


Figure 2-10 “New System Variable” dialog box

5) The new system variable “JAVA_HOME” under the “System variables” in window “Environment Variables”appears, as shown in Figure 2-11.

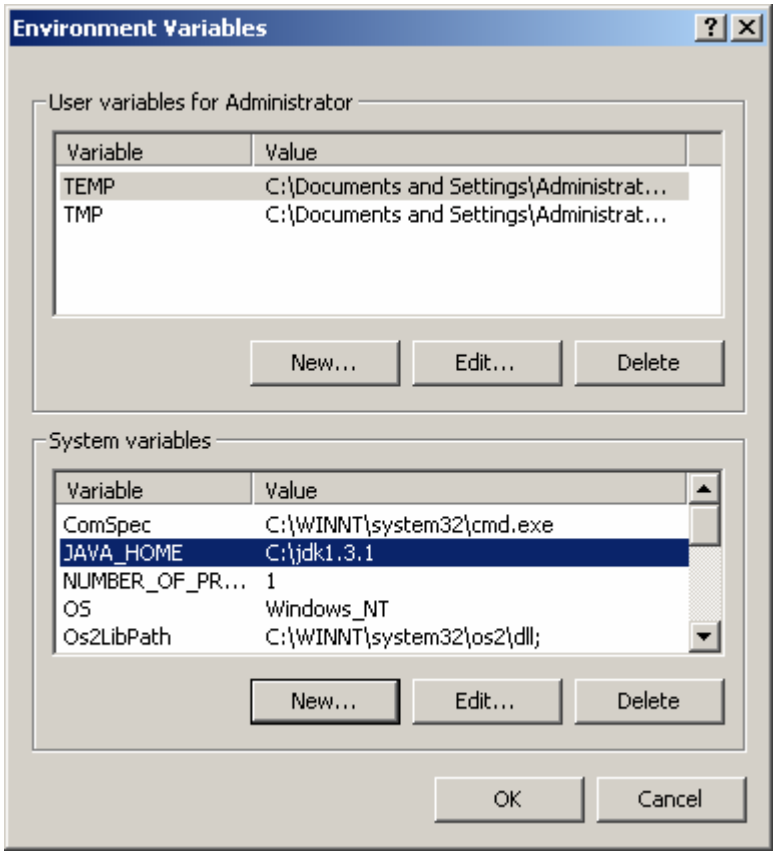


Figure 2-11 Newly added system variable

Click <OK>.

2.1.4 Installing RAS Software

The following describes specific installation steps:

1) Put the installation disk RemoteAccessInstallation in the CD-ROM. Double click the installation file InstallRemoteAccessServerInstallation.exe to install the RAS software.
2) The window "Welcome" is displayed, as shown in Figure 2-12. Click <Next>.

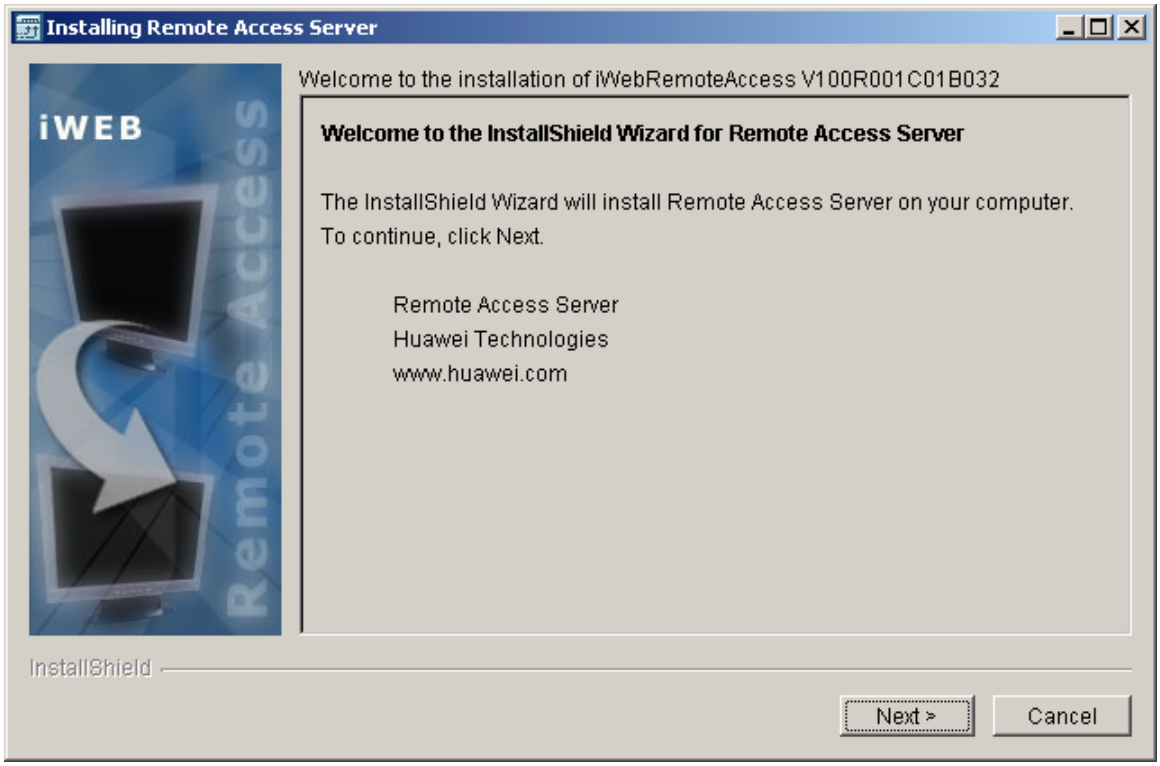


Figure 2-12 "Welcome" window

3) The window "Software License Agreement" is displayed, as shown in Figure 2-13. Select the option button "I accept the terms of this license agreement" if you accept the agreement. Click <Next>.

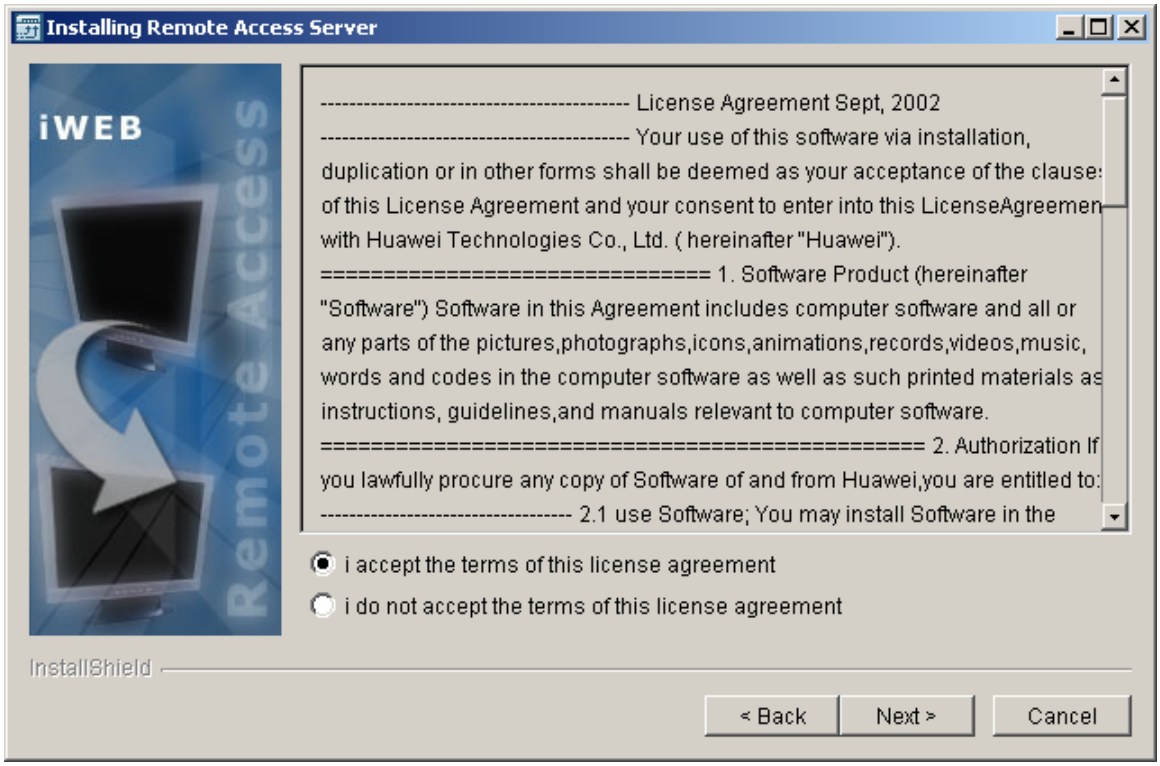

Installing Remote Access Server
iWEB
Remote Access
---------- License Agreement Sept, 2002
---------- Your use of this software via installation,
duplication or in other forms shall be deemed as your acceptance of the clause
of this License Agreement and your consent to enter into this LicenseAgreemen
with Huawei Technologies Co., Ltd. (hereinafter "Huawei").
========== 1. Software Product (hereinafter
"Software") Software in this Agreement includes computer software and all or
any parts of the pictures,photographs,icons,animations,records,videos,music,
words and codes in the computer software as well as such printed materials as
instructions, guidelines,and manuals relevant to computer software.
========== 2. Authorization If
you lawfully procure any copy of Software of and from Huawei,you are entitled to:
---------- 2.1 use Software; You may install Software in the
i accept the terms of this license agreement
i do not accept the terms of this license agreement
InstallShield
< Back
Next >
Cancel

Figure 2-13 “Software License Agreement” window

4) The directory selection window is displayed, as shown in Figure 2-14. Click <Browse> to select an installation directory. It is recommended to select the default installation directory C:\Remote Access\Server. Click <Next>.

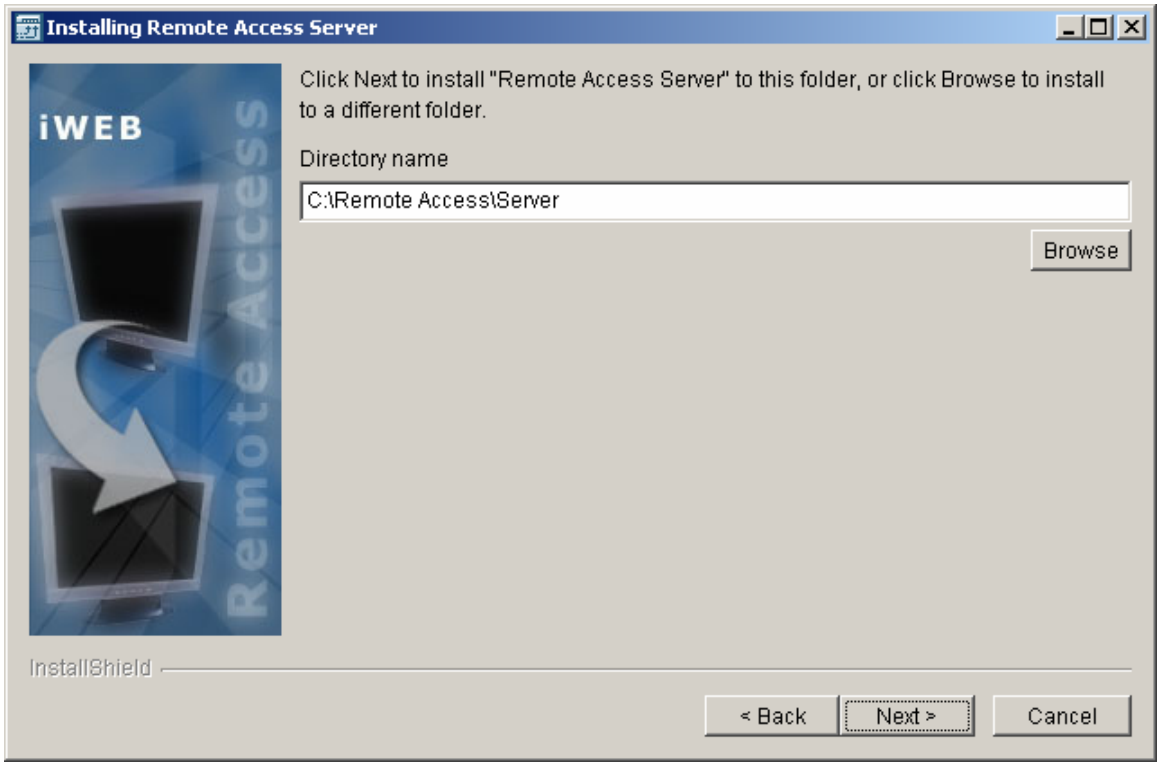


Figure 2-14 Directory selection window

5) The installation information confirmation window is displayed, as shown in Figure 2-15. Click <Next>.

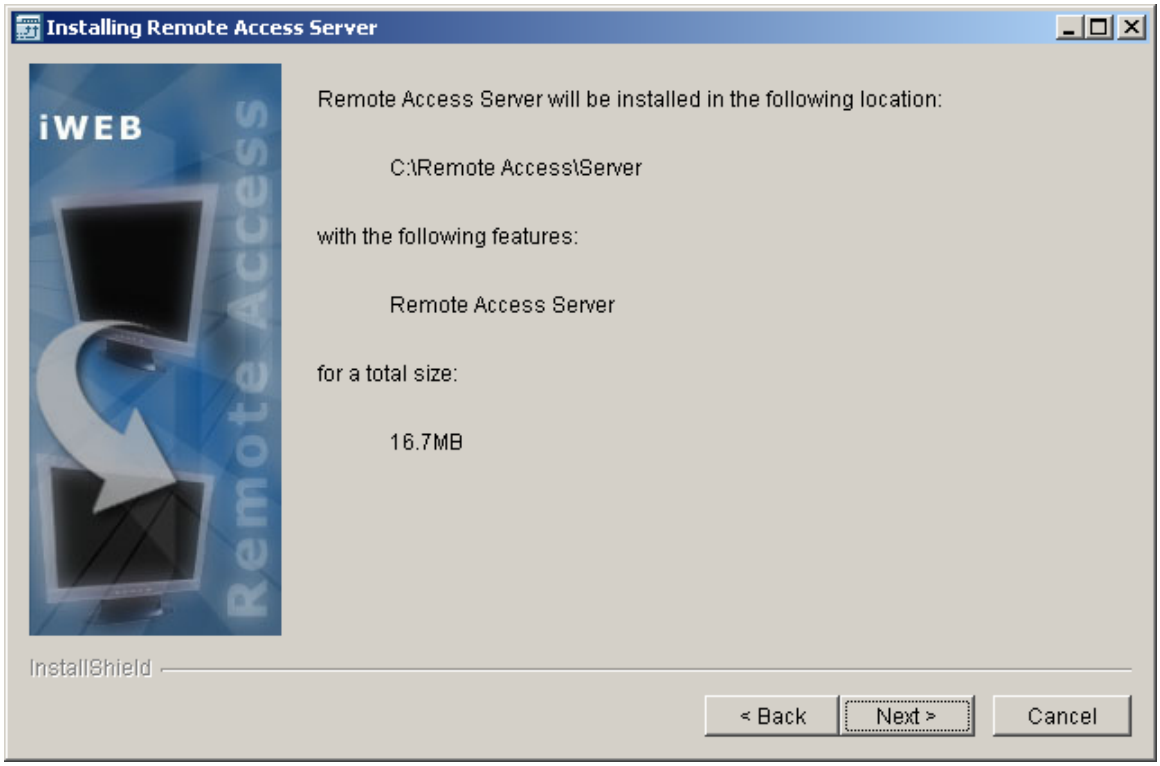


Figure 2-15 Installation information confirmation window

6) The window “Administrator Password Configuration” is displayed, as shown in Figure 2-16. Enter the password and click <Next>. If the system has been installed with the RAS software, follow step 7. If not, follow step 8 directly.

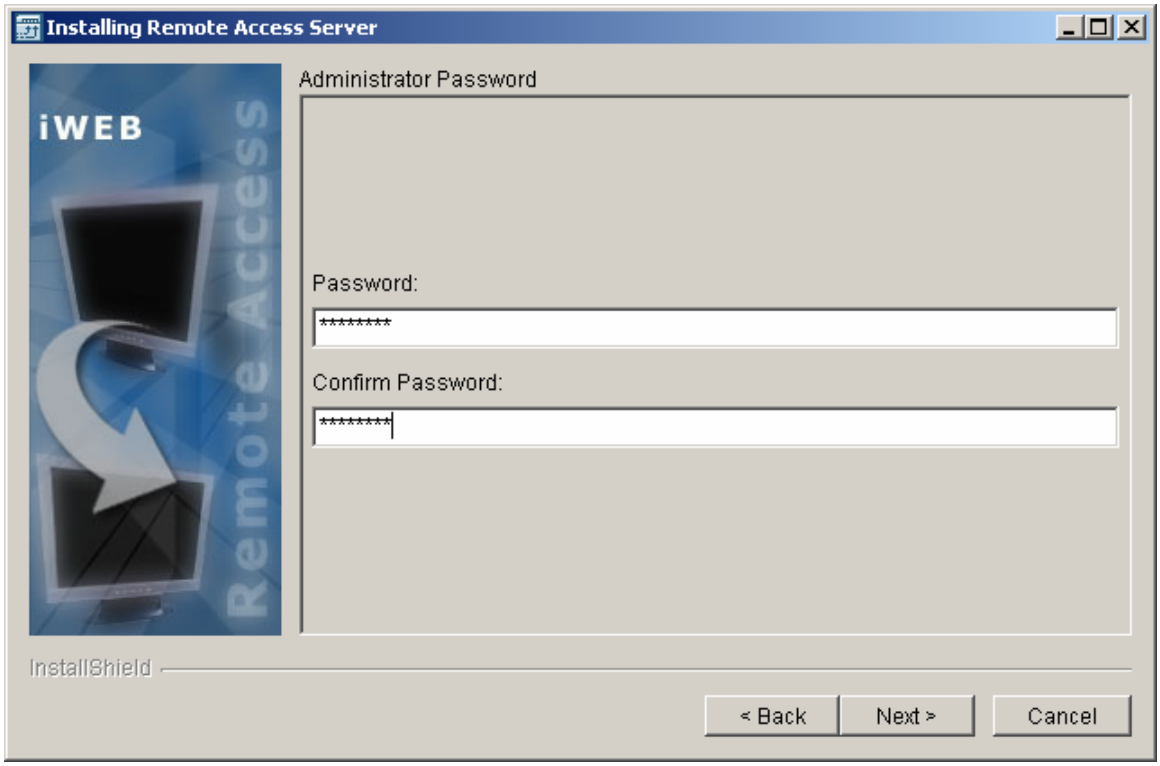


Figure 2-16 “Administrator Password Configuration” window

7) If the system has been installed with the RAS software, the window “Replace Existing Object" is displayed, as shown in Figure 2-17. The meanings of the three buttons are shown in Table 2-1. Click <Yes to All>; that is, replace all the current files.

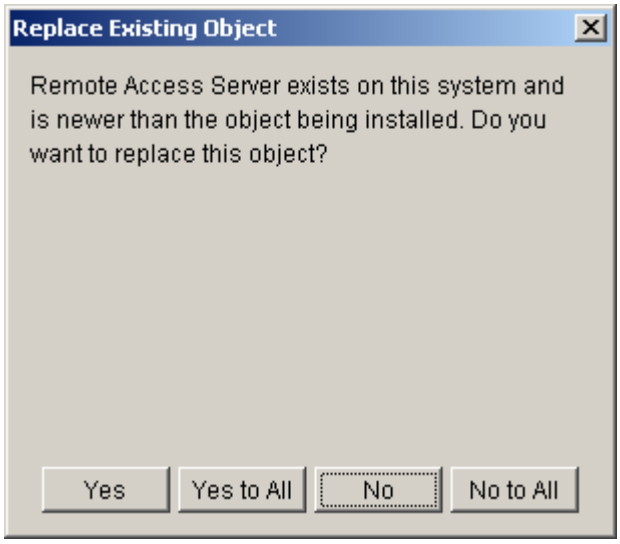

Replace Existing Object
Remote Access Server exists on this system and is newer than the object being installed. Do you want to replace this object?
Yes
Yes to All
No
No to All

Figure 2-17 “Replace Existing Object” window

Table 2-1 Button description in the window “Replace Existing Object”

Button	Description
<Yes>	To replace all the current files one by one
<Yes to All>	To replace all the current files at a time(recommended)
<No>	To keep all the current files one by one
<No to All>	To keep all the current files at a time

8) Files are copied to the installation directory. The window “Installation Successful” is displayed, as shown in Figure 2-18.

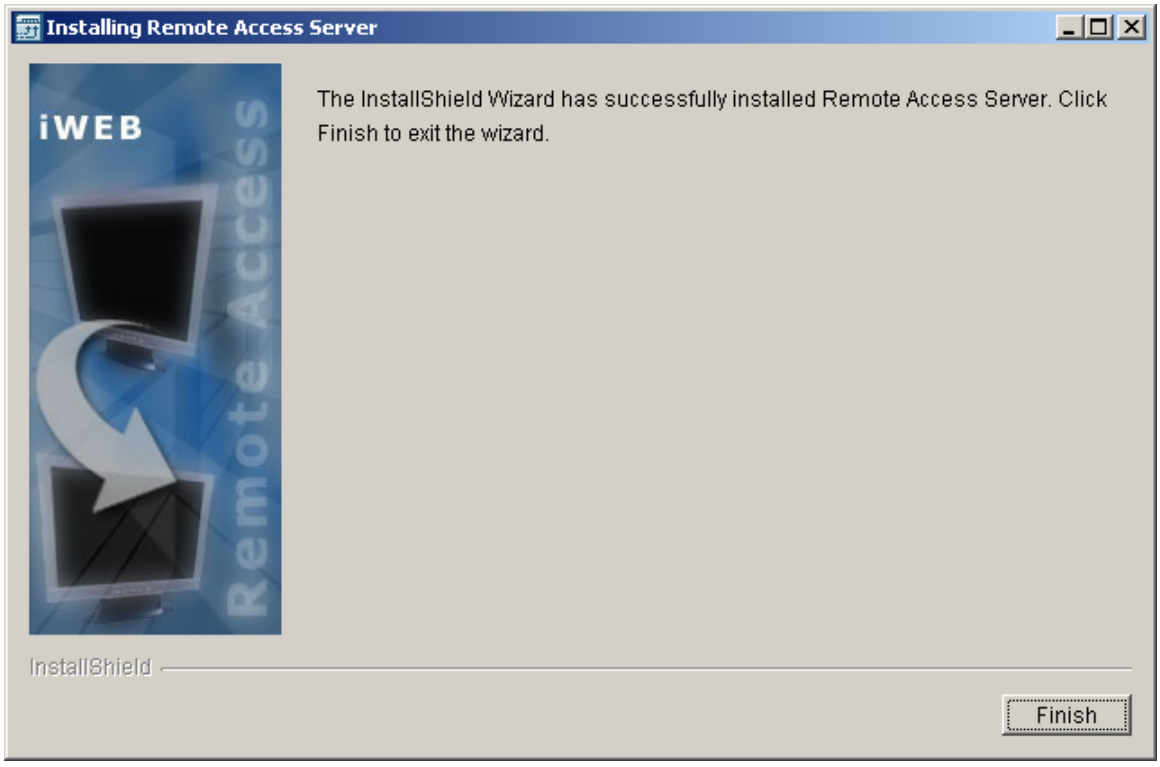

Installing Remote Access Server
iWEB
Remote Access
The InstallShield Wizard has successfully installed Remote Access Server. Click Finish to exit the wizard.
InstallShield
Finish

Figure 2-18 “Installation Successful” prompt window

Click <Finish>.

2.1.5 Check for RAS Software Installation

After the RAS software is installed, check whether the installation is successful in the following steps.

1) Under the installation directory, double click the file **run.bat** to run the background service.

2) Double click the IE icon on the desktop to open the IE browser, and enter http://localhost:9999/RemoteAccess in the address box. Press <Enter>. A login window is displayed, as shown in Figure 2-19.

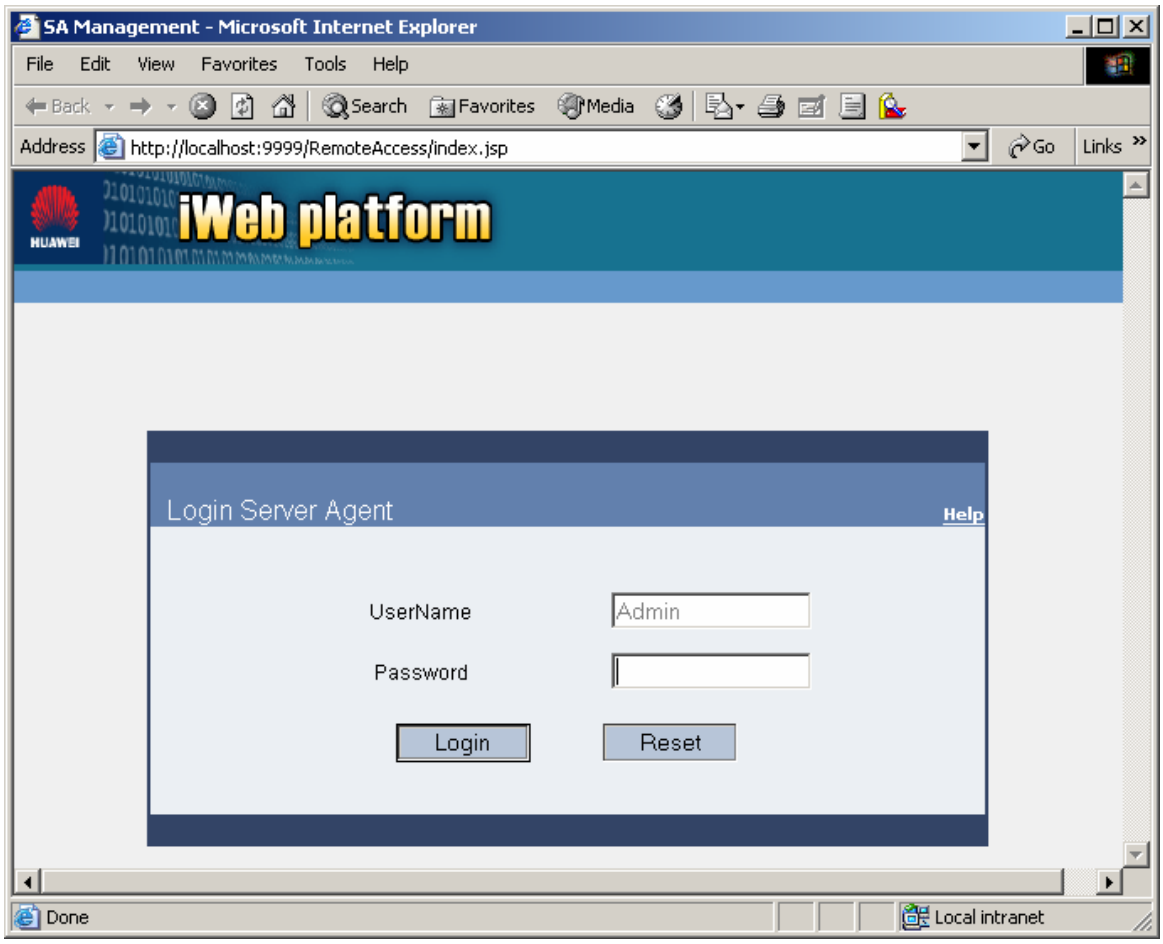


Figure 2-19 RAS login window

Note:

The default language should be set as English and the area should be set as English-speaking area on RAS. Meanwhile, the multi-language attribute must be set to English first; that is, by default IE menu and dialog box should be displayed in English. For the multi-language attribute of the RAS, refer to “3.2.2 Configuring Multi-Language Attribute”.

---

3) Enter the administrator password set during the RAS installation, and then click <Login>. If the login is successful, the server agent management window is displayed, as shown in Figure 2-20.

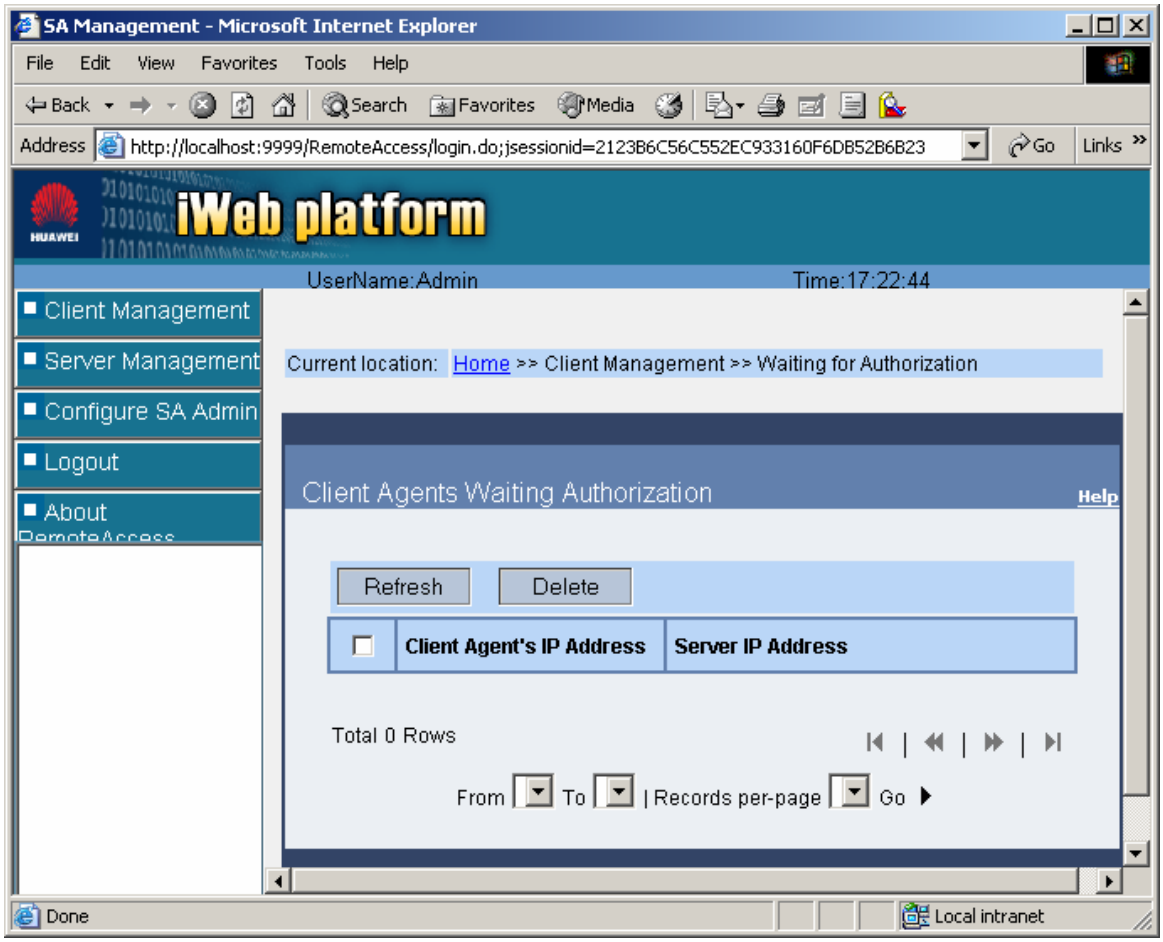


Figure 2-20 Server agent management window

2.1.6 Installing RAC Software

The installation steps of the RAC are the same as those of the RAS. Only installation programs and installation prompts are different. The installation program of the RAC is InstallRemoteAccessClientInstallation.exe. For details, refer to the RAS installation steps.

2.1.7 Check for RAC Software Installation

After the RAC is installed, check whether the installation is successful in the following steps.

1) Double click the “Remote Access Client” icon, then the “login” dialogue box is displayed, as shown in Figure 2-21.

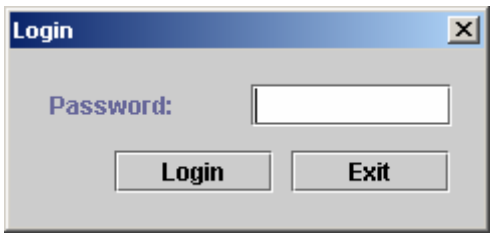


Figure 2-21 RAS login window

2) Enter the administrator password set during the RAC installation, and then click <Login>. If the login is successful, the RAC service window is displayed, as shown in Figure 2-22.

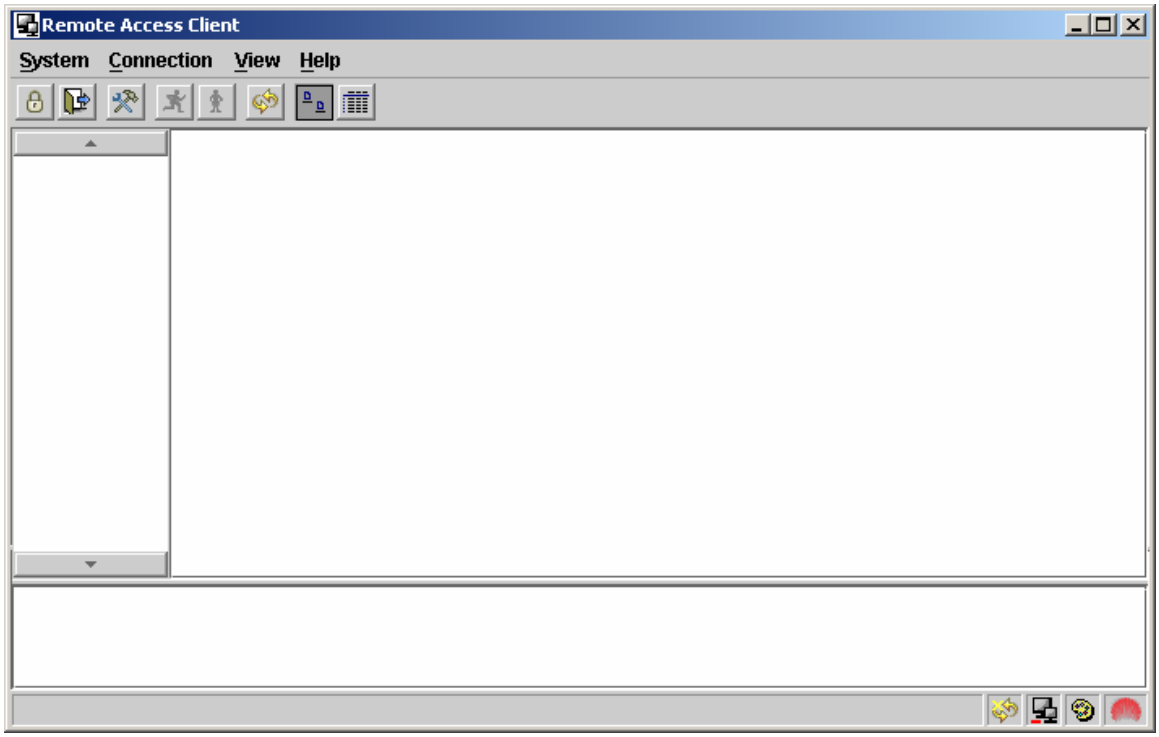


Figure 2-22 RAC service window

2.2 Uninstalling Software

The procedures for uninstalling the RAS software and the RAC software are the same, except that the prompts slightly are different. The following takes the RAS software as an example to introduce uninstalling steps.

1) Select [Start/Settings/Control Panel] to enter the control panel.
2) Click “Add/Remove Programs” in the control panel to enter the window “Add/Remove Programs”.
3) Select the program “Remote Access Client” and click <Change/Remove>, the window “Uninstaller” is displayed, as shown in Figure 2-23. Click <Next>.

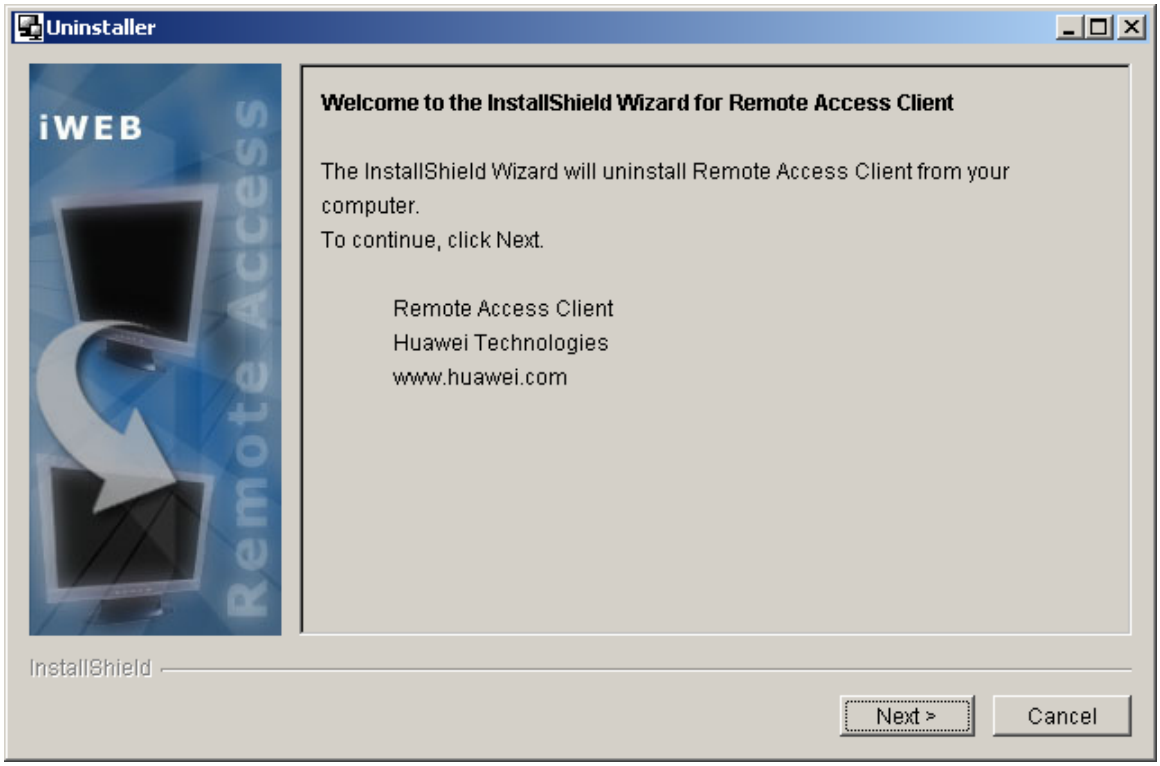


Figure 2-23 “Uninstaller” window

4) The window “Uninstallation Information Confirmation” is displayed, as shown in Figure 2-24. Click <Next>.

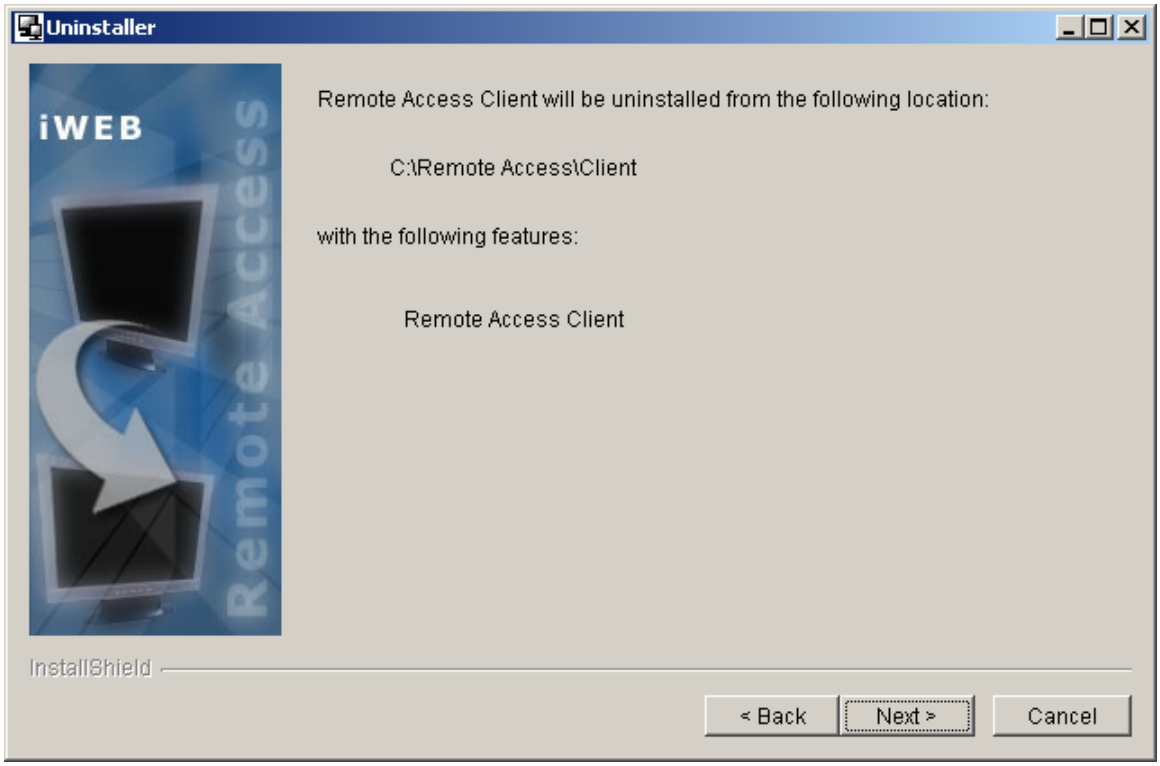


Figure 2-24 “Uninstallation Information Confirmation” window

5) The window “Remove Existing File” is displayed, as shown in Figure 2-25. The meanings of the following four buttons are listed in Table 2-2 Click <Yes to All>; that is, delete all the current files.

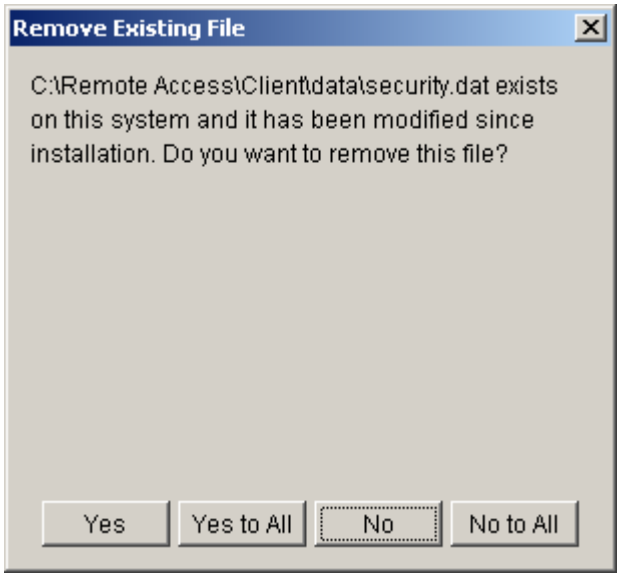

Remove Existing File
C:\Remote Access\Client\data\security.dat exists on this system and it has been modified since installation. Do you want to remove this file?
Yes
Yes to All
No
No to All

Figure 2-25 “Remove Existing File” window

Table 2-2 Button description in the window “Remove Existing File”

Button	Description
Click <Yes>	To delete the current file
Click <Yes to All>	To delete all the current files (recommended)
Click <No>	To keep the current file
Click <No to All>	To delete all the current files

6) The window “Uninstallation Finished” is displayed, as shown in Figure 2-26.

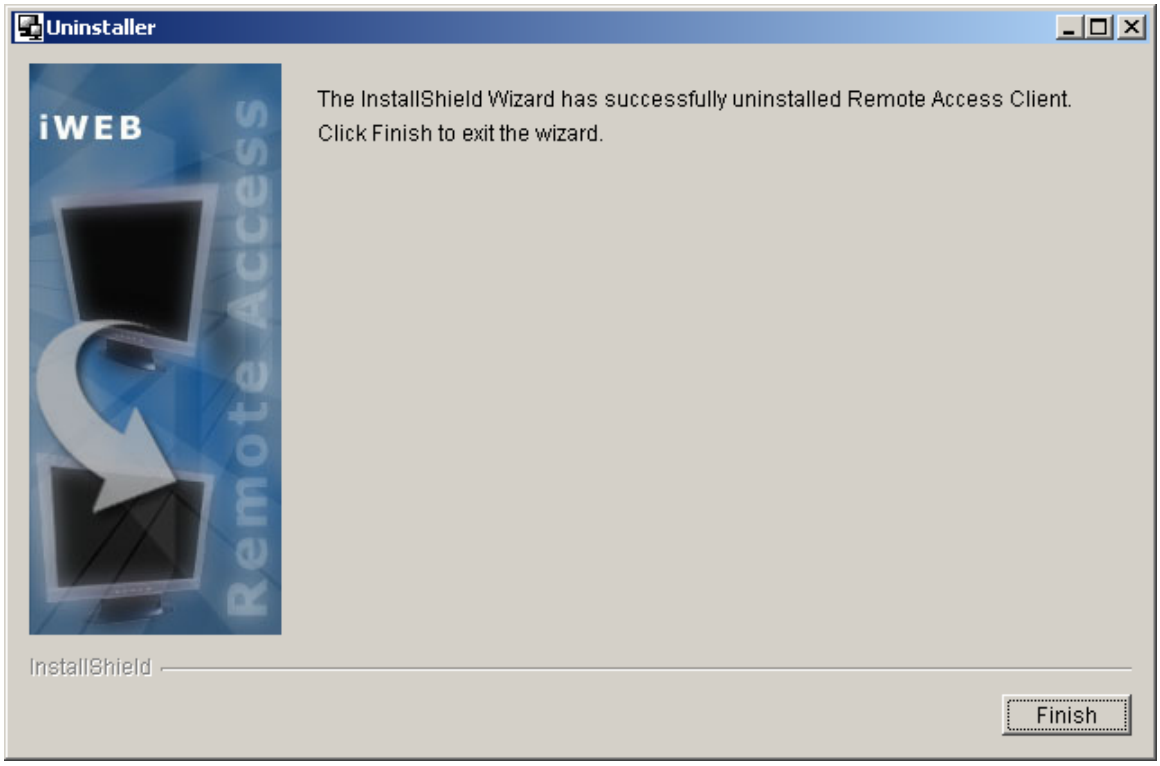


Figure 2-26 “Uninstalling Finished” window

7) Click <Finish>.

2.3 Frequently Asked Question in Software Uninstallation

I. Why does it appear that InstallShield searches JDK?

Reply: The possible reason is that the JDK version does not match the operating system. In this case install the correct JDK.

II. Why does the RAS or the RAC setup wizard display alarm information about disk space.

Reply: The disk space where the installation directory is located is insufficient. You can reselect an installation position, or exit the installation first to release disk space. Reinstall until the disk space meets requirements.

III. Why cannot start the RAS after the installation?

Reply: The possible reason is that the environment variable JAVA_HOME is not set to the installation directory of the JDK software. The following describes the processing steps:

1) Select the icon “My Computer” on the desktop. Right click and select <Properties> in the shortcut menu.
2) The window “System Properties” is displayed. Select the tab “Advanced” and click <Environment Variables>in it. Then the window “Environment Variables” is displayed.
3) In the “Environment Variables” window, check whether the variable “JAVA_HOME” exists in the “System Variables” and whether it is the installation directory of JDK.

- If the variable is not set yet, click <New> in the “System Variables”. Then enter “JAVA_HOME” in the “Variable Name” and enter the installation directory (the default is C:\jdk1.3.1) of JDK in the “Variable Value”. Click <OK>.
- If the variable has been set wrongly, click <Edit> in the “System Variables”. Then enter the installation directory of JDK in the “Variable Value”. Click <OK>.

Chapter 3 Operation Guide

3.1 Overview of Operation Guide

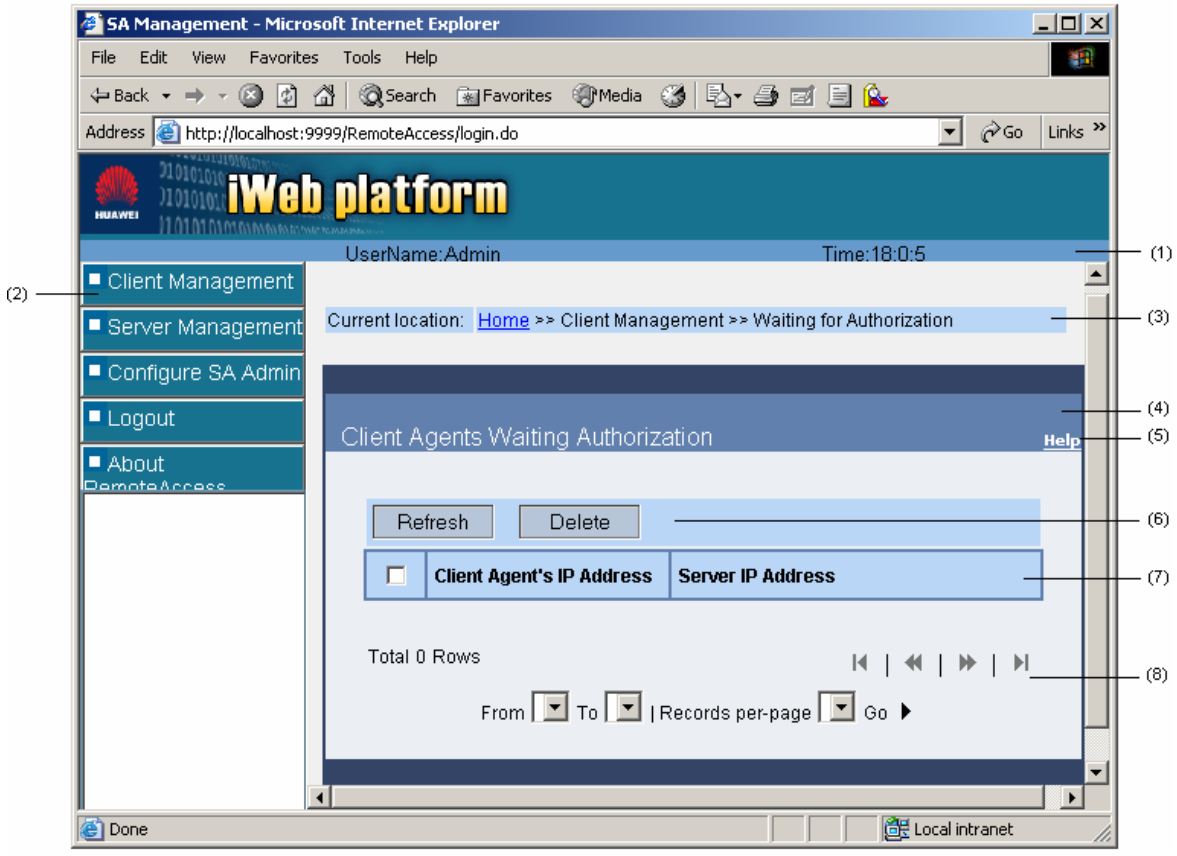
To make the whole system work normally, you must configure the corresponding data first after installing software of the iWeb remote maintenance access system. The data configuration of the iWeb remote maintenance access system consists of the RAS data configuration and the RAC data configuration. After data configuration, you can start the RAC and the RAS to establish connections for maintenance.

This chapter introduces the service interfaces of the RAS and the RAC, the data configuration of the RAS and the RAC, and other basic operations (including login and connection management) on the RAS and the RAC. At last, the chapter takes an example to illustrate the working process of the iWeb remote maintenance access system.

3.2 Introduction to Service Interfaces

3.2.1 RAS Service Interface

The RAS service interface is shown in Figure 3-1.



(1) User information (2) Navigation menu (3) Page information
(4) Operating window information (5) Help button (6) Operating command button
(7) Operating object information (8) Information browse button

Figure 3-1 RAS service interface

In the above figure, the RAS service interface consists of the following four parts.

I. User Information

It displays the RAS user name and login time.

II. Navigation Menu

It displays various operation menus of the RAS in the mode similar to navigation tree. Click an item on a menu, and the corresponding window will pop up in the right window of the service interface. There are submenus under some menus of the navigation menu. Subnodes are spread when you click the corresponding node.

III. Page Information

It displays the location of the current page under the navigation menu.

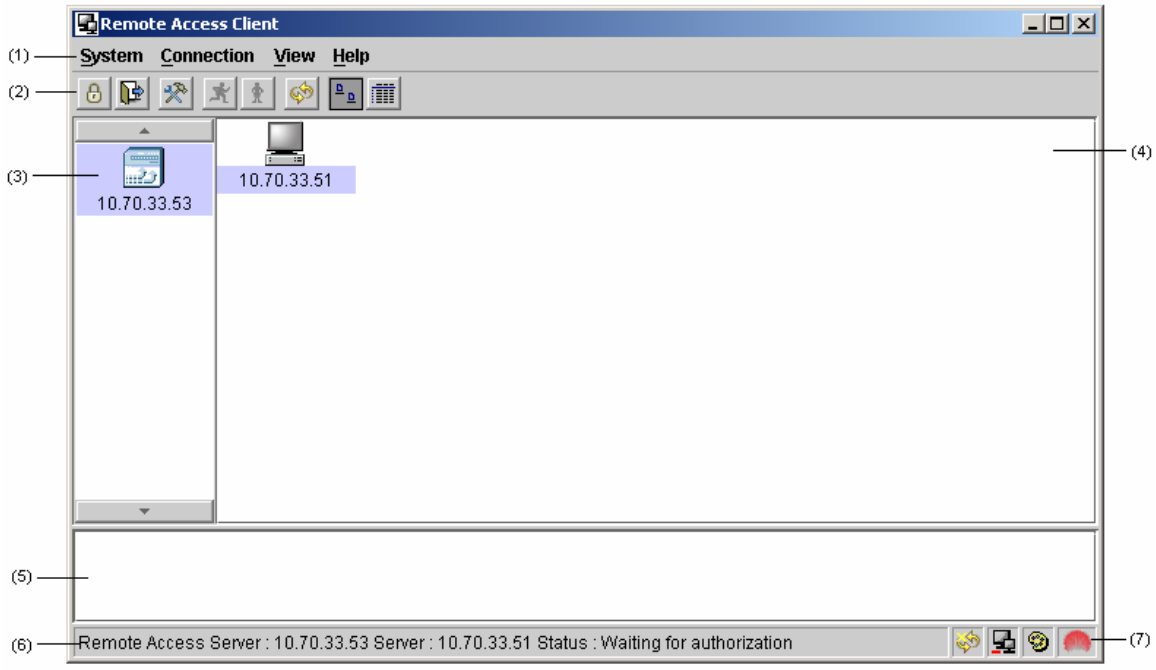
IV. Operating Window

Specific configuration and operation of the RAS are implemented in this window. The window includes the following:

- Operating window information, which describes operation types.
- Help button, which opens online help in the RAS service interface.
- Operating command buttons, which select specific operating command types. Sometimes, the operating command is displayed below operating object information.
- Operating object information, which lists operating objects or describes operating object information.
- Information browse buttons, which browse operating object information, including operating buttons about record selection and page reversal.

3.2.2 RAC Service Interface

The service interface of the RAC is shown in Figure 3-2.



(1) Main menu (2) Tool bar (3) RAS list
(4)Equipment server list (5) Output window (6) Connection status bar
(7) Operating shortcut key

Figure 3-2 RAC service interface

In the above figure, the RAC service interface consists of the following seven parts.

- 1. Main menu
- It provides all operation menus of RAC.
- Tool bar
- It provides shortcut icons about operating RAC.
- RAS list window
- It displays IP addresses of all RASs connected with local RAC.
- Equipment server list window

- It displays IP addresses of servers connected with local RAC under each RAS.
- Output window
- It is to exports the RAC operation results.
- Status bar,
- It displays the status of the selected connection.
- Shortcut icons
- Including shortcut icons of some operation, it is to refresh records automatically, check the color display setting of the connection and check the version number of the iWeb remote maintenance access system.

The meanings of the shortcut icons in Figure 3-2 are shown in Table 3-1.

Table 3-1 Shortcut icons in the RAC service interface

Icon	Meaning
	Locks the RAC service interface.
	Closes the RAC service interface.
	Opens proxy and security setting window.
	Activates established maintenance connections that are not in the working status.
	Deactivates maintenance connections that are in the working status.
	Refreshes all the connection statuses.
	Displays all the connections in the icon mode.
	Displays connection information in details.
	Sets automatic refresh parameters. Double click to open it.
	Displays the current connection status. The “-” in the icon shows different colors, which represent different connection statuses.
	Displays the relationship between display colors and connection statuses. Click it to open the corresponding description, and then click to close it.
	Displays the version information of the iWeb remote maintenance system. Double click it to open the version information.

3.3 RAS Data Configuration

The RAS data configuration includes:

- Configuring IP address and ports.
- Configuring multi-language attribute
- Configuring log functions
- Configuring connection instances
- Configuring server access strategy

Configuring server access strategy includes configuring server types and configuring server instances.

3.3.1 Configuring IP Address and Ports.

If an RAS has multiple IP addresses, you need to bind the RAS software with one of these IP addresses. Otherwise, the RAC cannot connect the RAS. Also, port numbers of HTTP and HTTPS must be set so that remote maintenance can traverse proxy servers and firewalls.

Note:

- The HTTP port number is 9999 by default.
- The HTTPS port number is 8443 by default.

The following describes the specific steps in configuring IP address and ports.

1) Enter the RAS installation directory. The default is C:\Remote Access\Server.
2) Use the text editor to open the file **server.xml** under the directory **conf.**
3) Set IP address (the corresponding parameter item is address) and ports (the corresponding parameter item is Port) based on needs.

The following takes an example to illustrate the configuration about IP address and ports. Parameters or marks that must be modified in the example are overstriking and italic.

The IP address is set to **10.121.1.3**, HTTP port number is set to **9999**, and HTTPS port number is 8443.

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
               port="9999" minProcessors="5" maxProcessors="75"
               enableLookups="true" redirectPort="8443"
                    address="10.121.1.3"
               acceptCount="10" debug="0" connectionTimeout="60000"/>
<Connector className="org.apache.catalina.connector.http.HttpConnector"
               port="8443" minProcessors="5" maxProcessors="75"
               enableLookups="true"
               address="10.121.1.3"
               acceptCount="10" debug="0" scheme="https"
               secure="true">
```

3.3.2 Configuring Multi-Language Attribute

The RAS supports the multi-language attribute. Menus, dialog boxes and pages are displayed according to the set language categories and encode types in the IE service window.

The following describes the specific steps in configuring multi-language attribute.

1) Double click the icon “Internet Explorer” on the desktop to open the IE browser.
2) Select [Tools/Internet Options]. The window “Internet Options” is displayed, as shown in Figure 3-3.

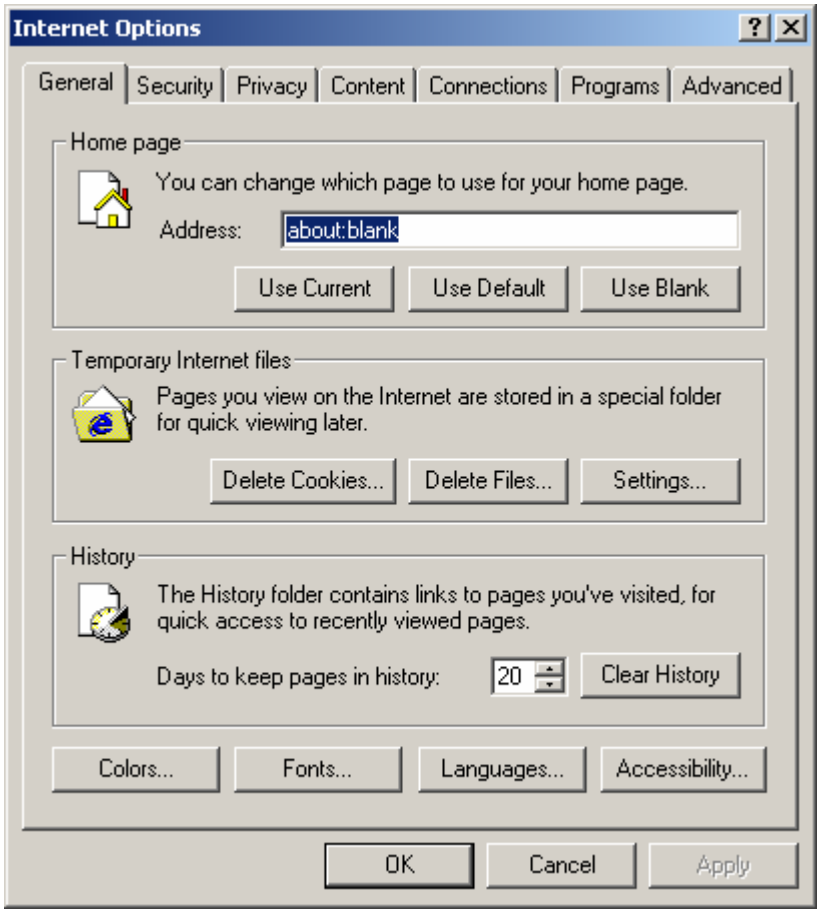


Figure 3-3 “Internet Options” window

3) Click <Languages> in the window “Internet Options”. The window “Language Preference” is displayed, as shown in Figure 3-4.

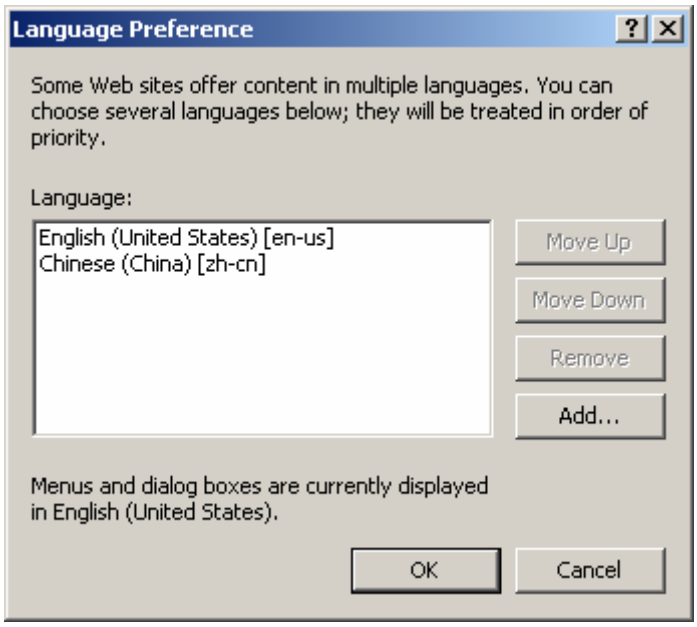

Language Preference
Some Web sites offer content in multiple languages. You can choose several languages below; they will be treated in order of priority.
Language:
English (United States) [en-us]
Chinese (China) [zh-cn]
Move Up
Move Down
Remove
Add...
Menus and dialog boxes are currently displayed in English (United States).
OK
Cancel

Figure 3-4 "Language Preference" window

4) Click <Add> in the window "Language Preference". The window "Add Language" is displayed, as shown in Figure 3-5.

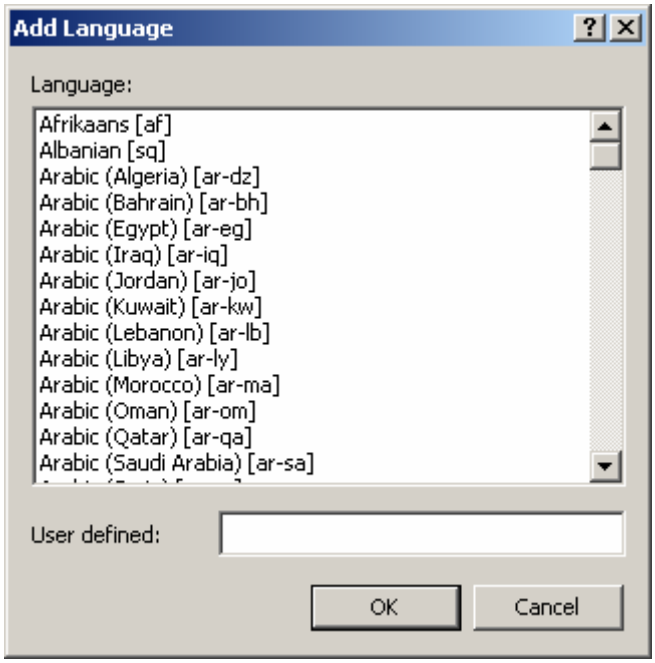


Figure 3-5 "Add Language" window

5) In the above figure, select a language to be used in the IE service window and click <OK>. Then the language is added to the window "Language Preference", as shown in Figure 3-6. Click <OK>.

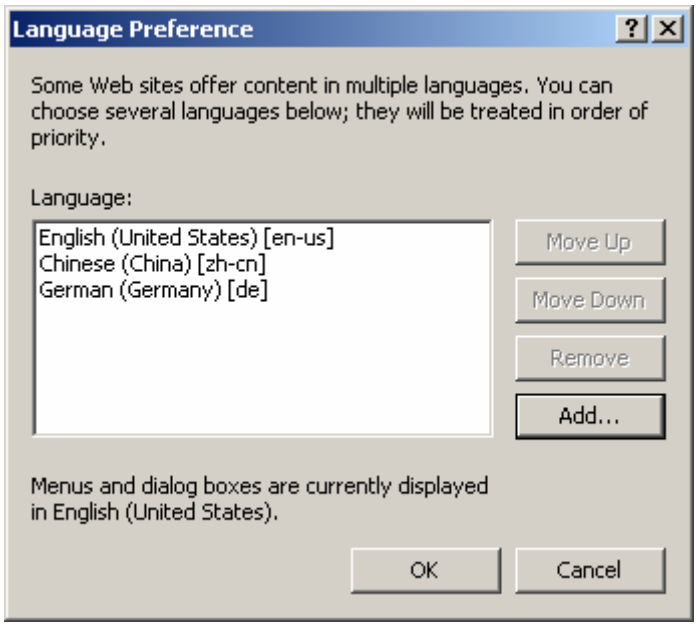

Language Preference
Some Web sites offer content in multiple languages. You can choose several languages below; they will be treated in order of priority.
Language:
English (United States) [en-us]
Chinese (China) [zh-cn]
German (Germany) [de]
Move Up
Move Down
Remove
Add...
Menus and dialog boxes are currently displayed in English (United States).
OK
Cancel

Figure 3-6 Adding a new language option

🕮 **Note:**

- In the window “Language Preference” , menus and dialog boxes are displayed in a language according to the precedence order (priority) of languages. More higher a language is located, more higher its priority is. In the above figure, menus and dialog boxes are displayed in English preferentially.
- Select a language, and click <Move Up> or <Move Down> to change its position in the window. By doing so, its priority changes.

---

6) Open the IE browser. Right click and select an encode in the shortcut menu. Content formats in the IE page vary with encode formats. It is recommended to adopt the default encode format to display the IE page.
7) Restart the IE browser.

3.3.3 Configuring Log Functions

The RAS log function consists of application layer log function and access layer log function. The former describes production application details (including maintenance operation records); the latter records lower layer communication conditions (including connection statuses). By modifying the configuration file, you can determine whether to start the above log functions.

The following describes operation steps in configuring log functions.

1) Enter the RAS installation directory. The default is C:\Remote Access\Server.

2) Use the text editor to open the file **logconfig.xml** under the directory conf.
3) Start or close various log functions based on needs. The label corresponding to the log function switch is <LogOption>…</LogOption>. If you set the above label to <LogOption>Enable</LogOption>, it indicates starting log functions. If you set the label to <LogOption>Disable</LogOption>, it indicates closing log functions. The default is set to start various functions.

The following is an example of the application layer log function configuration. The overstriking and italic part is the log function configuration option.

```
<!--  Extend System  -->
<ApplicationInfo ApplicationName="iWebExtend">
    <LogOption>Enable</LogOption>
    <File>
        <FileName>RemoteAccessServer.txt</FileName>
        <DirectoryPath>./logs/ra</DirectoryPath>
        <Layout>DebugPattern</Layout>
        <MaximumSize>2000</MaximumSize>
        <RollingFile>NO</RollingFile>
    </File>
    <Severity>ALL</Severity>
</ApplicationInfo>
```

The following is an example of the access layer log function configuration. The overstriking and italic part is the log function configuration option.

```
<!--  Access Layer  -->
<ApplicationInfo ApplicationName="Access Layer Framework">
    <LogOption>Enable</LogOption>
    <File>
        <FileName>AccessServer.txt</FileName>
        <DirectoryPath>./logs/ra</DirectoryPath>
        <Layout>DebugPattern</Layout>
        <MaximumSize>2000</MaximumSize>
        <RollingFile>NO</RollingFile>
    </File>
    <Severity>ALL</Severity>
</ApplicationInfo>
```

3.3.4 Configuring Connection Instances

Configuring connection instances is to determine maintenance connections which can be done on RAS. Here the maintenance connection means the connection from the RAC to servers. It consists of:

- Adding connection instances;
- Deleting connection instances;

- Refreshing connection statuses;
- Canceling connection authentication.

I. Adding Connection Instances

The following describes the specific steps in adding a connection instance.

1) Double click the file **run.bat** under the installation directory to run the background service. Or select [Start/Programs/Remote Access/Start Remote Access Server] to run the background service.
2) Double click the IE icon to open the IE browser. Enter http://localhost:9999/RemoteAccess in the address box, in which localhost means the local host and 9999 means the HTTP port. Press <Enter>. A login window is displayed, as shown in Figure 3-7.

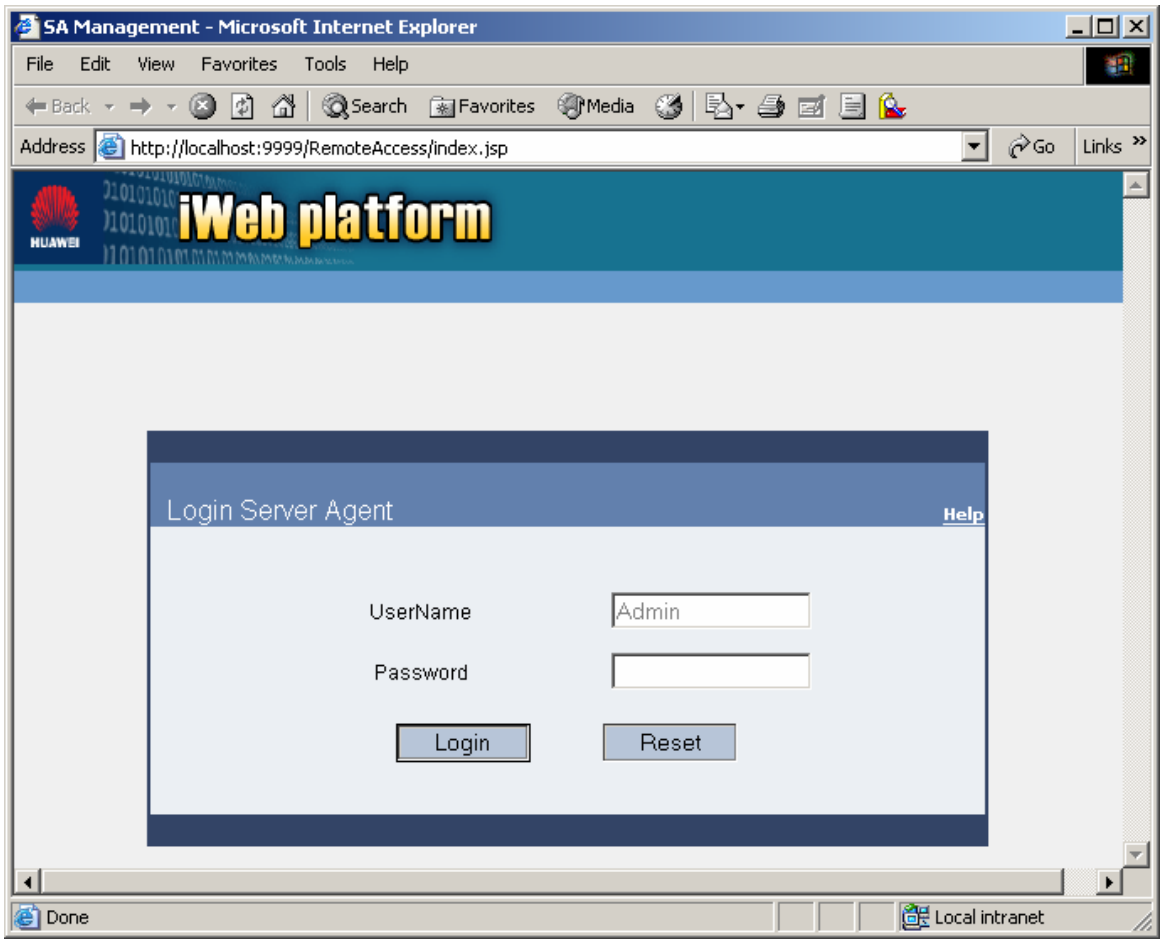


Figure 3-7 Login window in the RAS service interface

Note:

You can log in the RAS from another computer without the RAS software installed, and enter http://RASIP:9999/RemoteAccess in the address box, in which RASIP means the IP address of a computer with RAS installed. For example, in the http://10.70.33.53:9999/RemoteAccess, 10.70.33.53 means the IP address of a computer with the RAS installed.

3) Enter the administrator password and then click <Login>. If the login is successful, the RAS service interface is displayed, as shown in Figure 3-8.

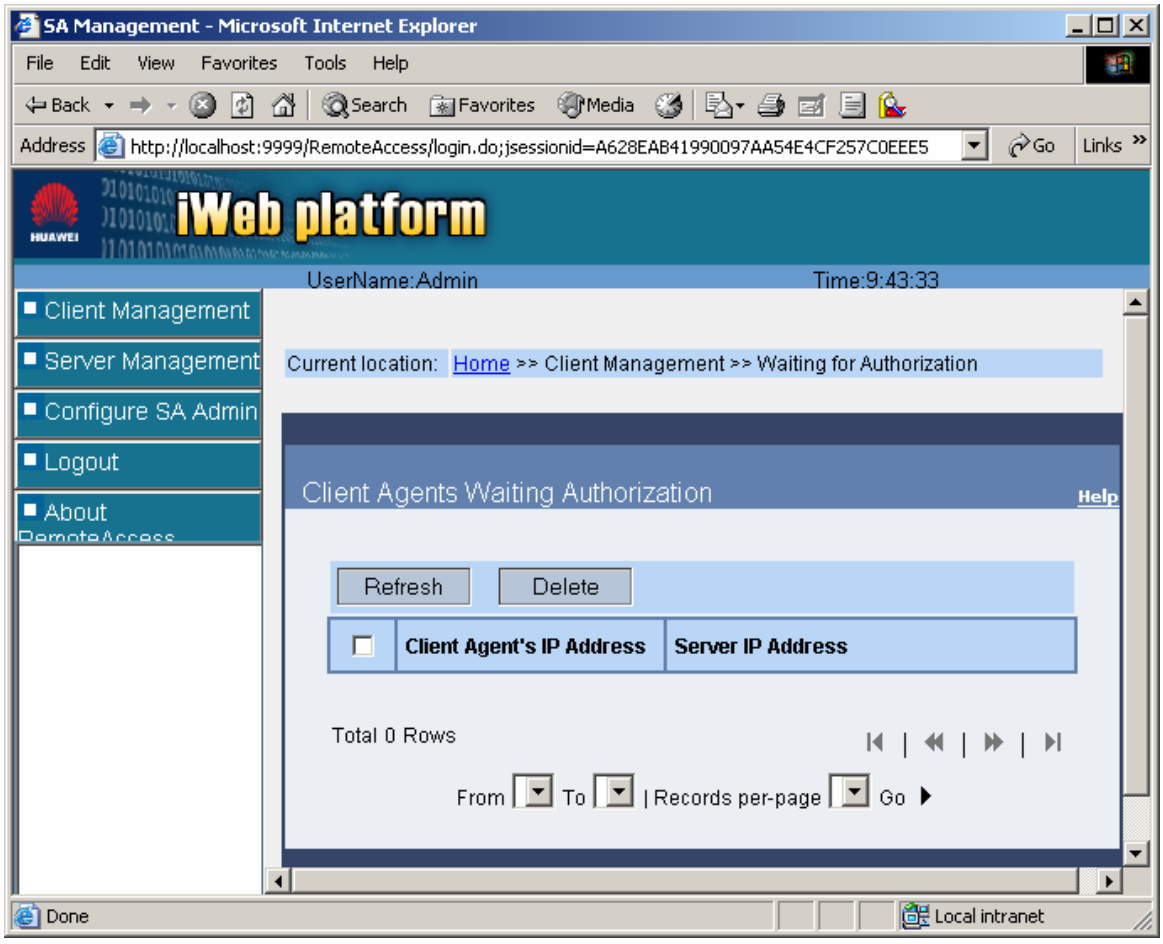


Figure 3-8 RAS service interface

4) In the RAS service interface, click the menu item “Client Management” under the left navigation menu, then click the submenu “Configured Client”. The window “View Configured Client Session List” is displayed on the right, as shown Figure 3-9.

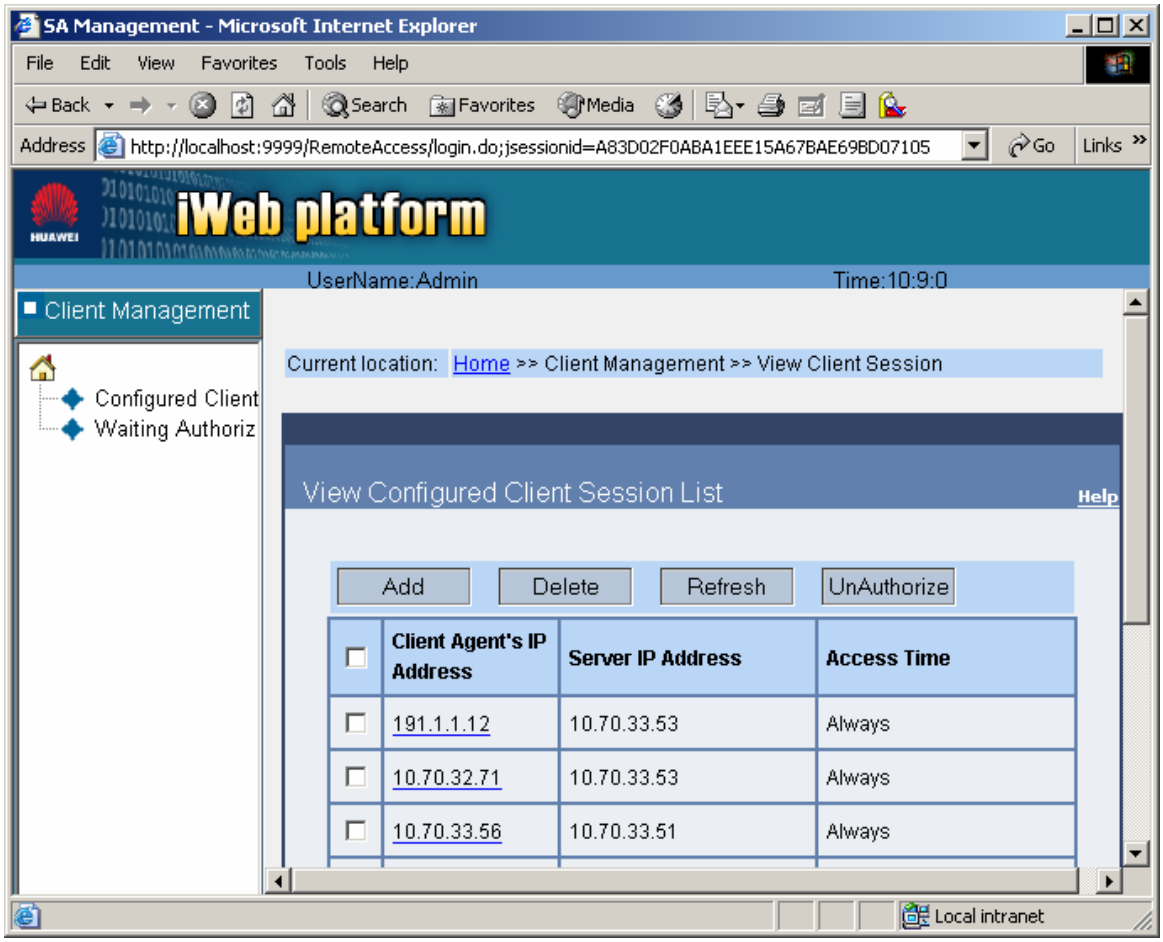


Figure 3-9 "View Configured Client Session List" window

5) Click <Add>. The window "Add Client Session Information" is displayed on the right of the interface, as shown in Figure 3-10.

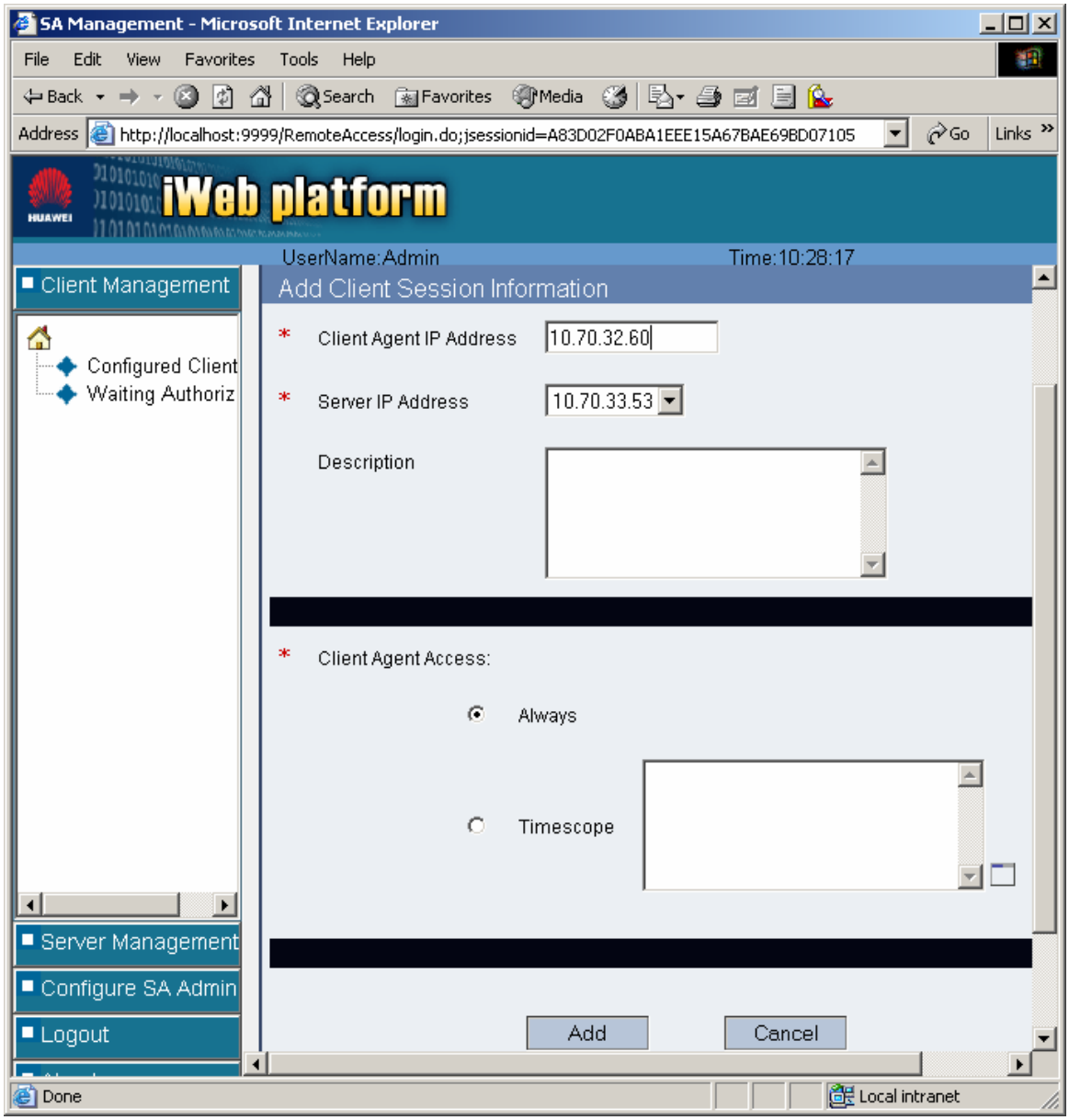


Figure 3-10 “Add Client Session Information” window

- Enter the IP address of the RAC in [Client Agent IP Address].
- Select an IP address of an server to be maintained remotely in the “Server IP Address”.
- Add a description of the RAC in the “Description” box.
- Select a connection mode between RAC and RAS in the “Client Agent Access” box based on needs. If you select “Always”, the connection between RAS and RAC is not time-limited. If you select “Timescope”, click the time setting button beside it and select a time range.

6) After filling in related information, click <Add>. A connection instance can be added in the “Client Session List”, as shown in Figure 3-11.

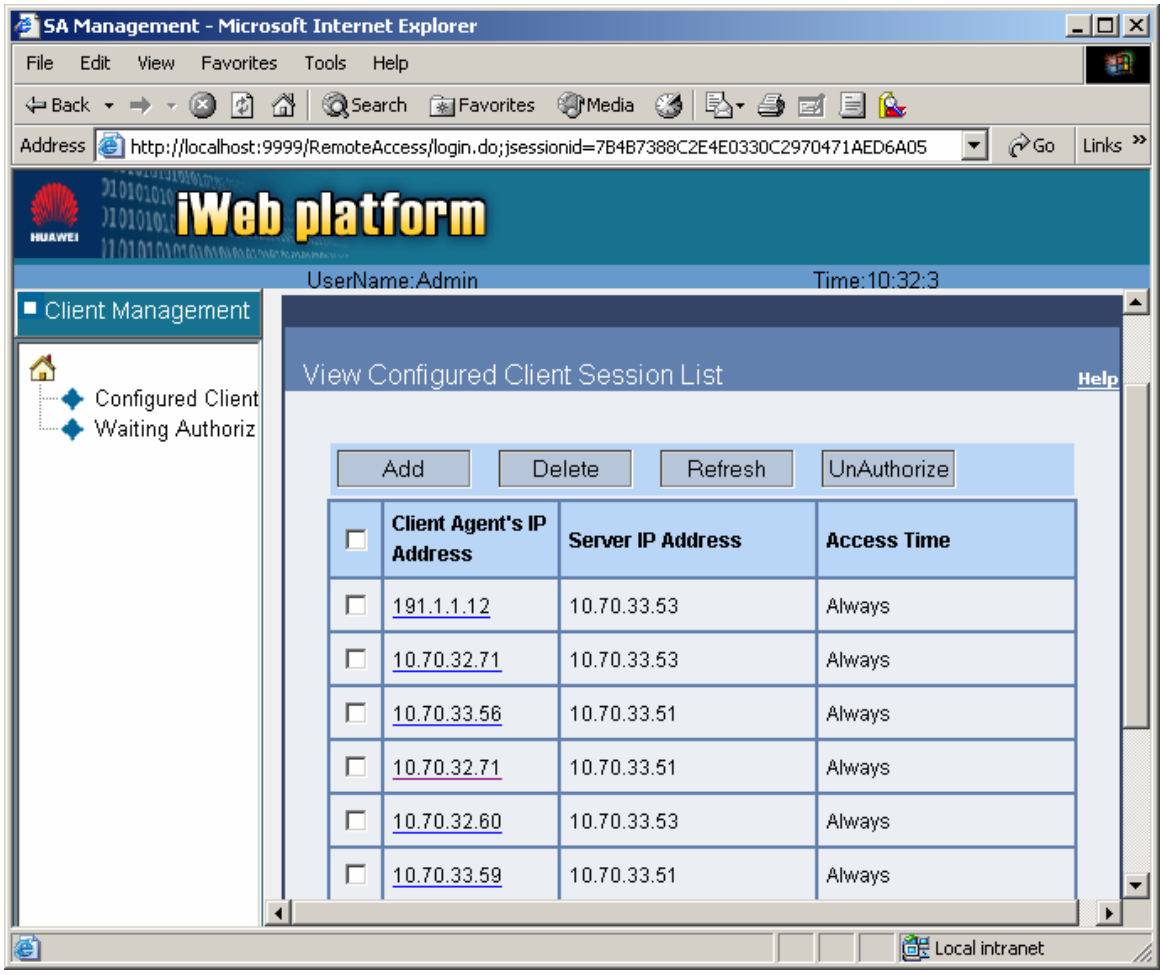


Figure 3-11 Upgraded “Client Session list”

Note:

If a connection has been added from an RAC to a server, the RAC shall check the request and approve the authentication when the RAC sends a connection request connecting the same server to the RAS.

II. Deleting Connection Instances

If you want to delete a connection instance, select it in the “Client Session List”; that is, tick the checkbox before the instance and click <Delete>. A prompt is displayed, as shown in Figure 3-12.

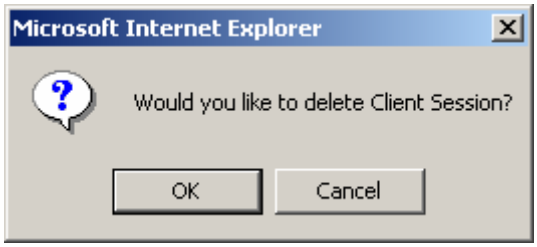


Figure 3-12 Prompt information of deleting a connection instance

Click <OK> to delete the connection.

III. Refreshing Connection Statuses

Table 3-2 shows the relationship between display colors and connection statuses in the “Client Session List”.

Table 3-2 Relationship between colors and connection statuses

Color	Connection status
Grey	The connection has been configured in the list, but RAC does not send the connection request.
Sky blue	The connection has been configured in the list; the connection request from RAC has been initiated and the RAS authentication is passed. However, the connection is still in the inactivated state.
Green	The connection has been configured in the list; the connection request from RAC has been initiated and the RAS authentication is passed. The connection is in the working state.

Click <Refresh> to refresh the color display of a connection instance.

IV. Canceling RAC Authentication

When an RAC sends a connection request to an RAS and passes the authentication for the first time, the RAS turns the color of the instance in the “Client Session List” to sky blue (refer to Table 3-2) and records the authentication result. When the RAC resends a connection request, the RAS will not authenticates the request.

To ensure the remote maintenance security, some authentication records must be deleted; that is, the RAS should authenticates requests from the RAC again. Specific steps: Select a corresponding instance in the window “View Configured Client Session List” and click <UnAuthorize>. A prompt is displayed, as shown in Figure 3-13. Click <OK>. The color of the instance turns grey (refer to 3-2) in “Client Session List”.

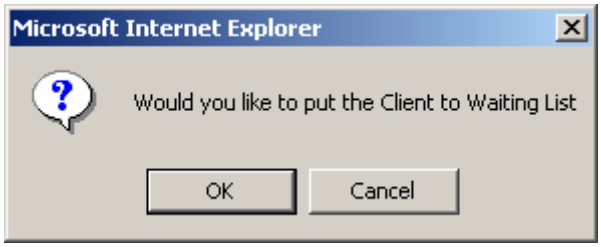


Figure 3-13 Prompt information of canceling a connection authentication

3.3.5 Configuring Server Types

Configuring server types means configuring server types to be maintained in the iWeb remote maintenance access system. It includes adding server types and deleting server types.

I. Adding Server Types

1) Refer to 3.2.4 “Configuring Connection Instances” to enter the RAS service interface.
2) In the RAS service interface, click the menu item “Server Management” under the left navigation menu, and then click the submenu “Server Types”. The window “View Server Types” is displayed on the right, as shown Figure 3-14.

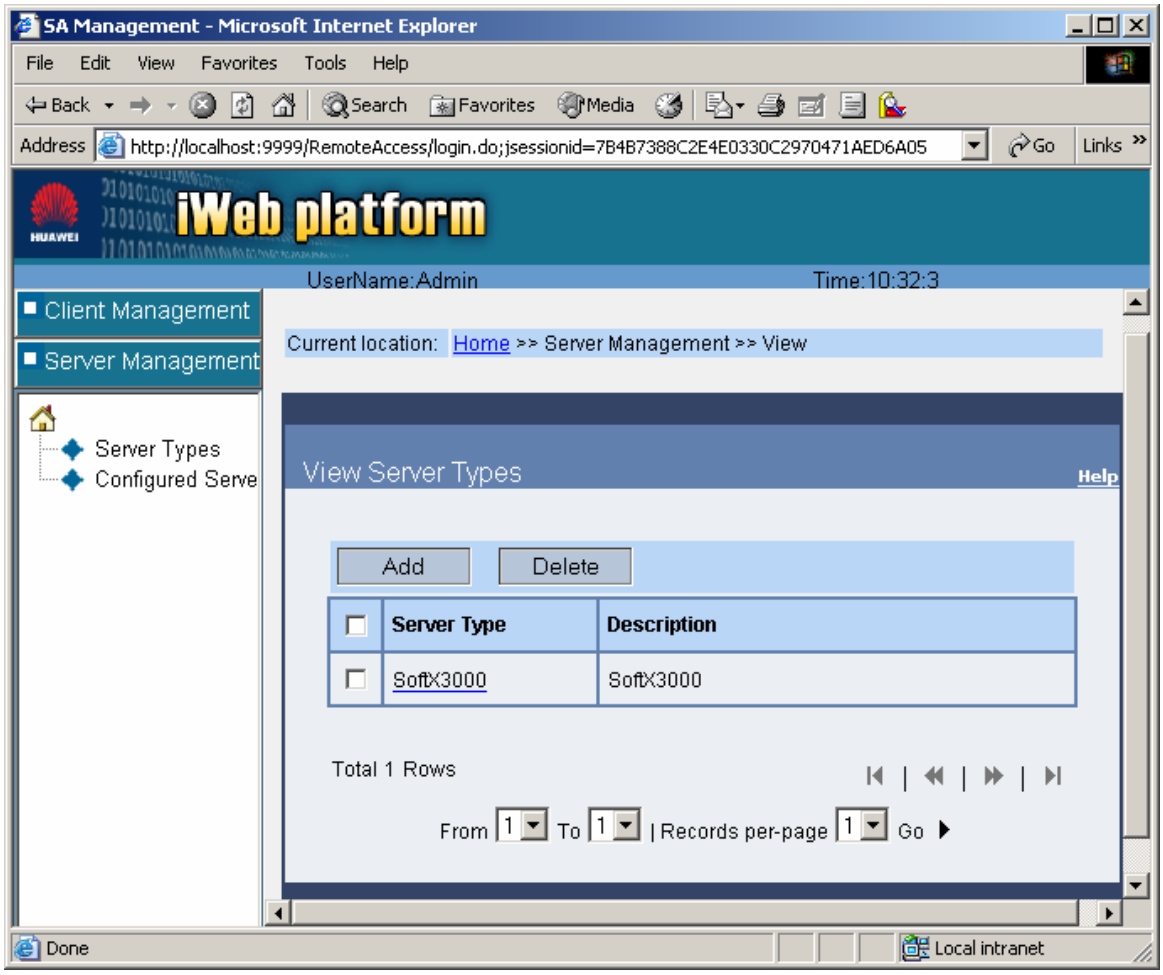


Figure 3-14 “View Server Types” window

3) Click <Add>. The window “Add Server Type” is displayed on the right of the interface, as shown in Figure 3-15.

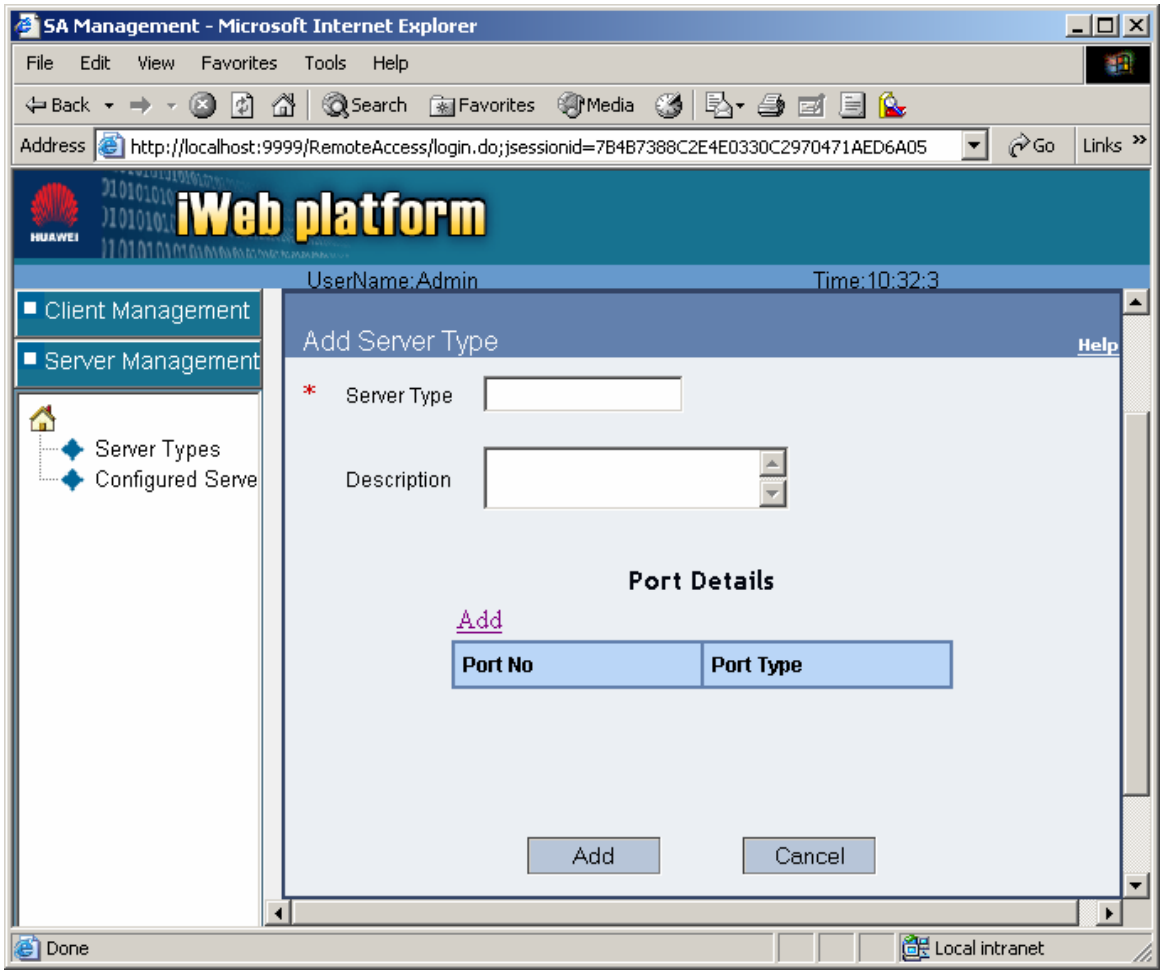


Figure 3-15 “Add Server Type” window

- Add a server type to be maintained in the “Server Type” box.
- Describe the server type in the “Description” box.
- Click <Add> in the window “Port Details”. The window “Add Port” is displayed on the right of the interface, as shown in Figure 3-16.

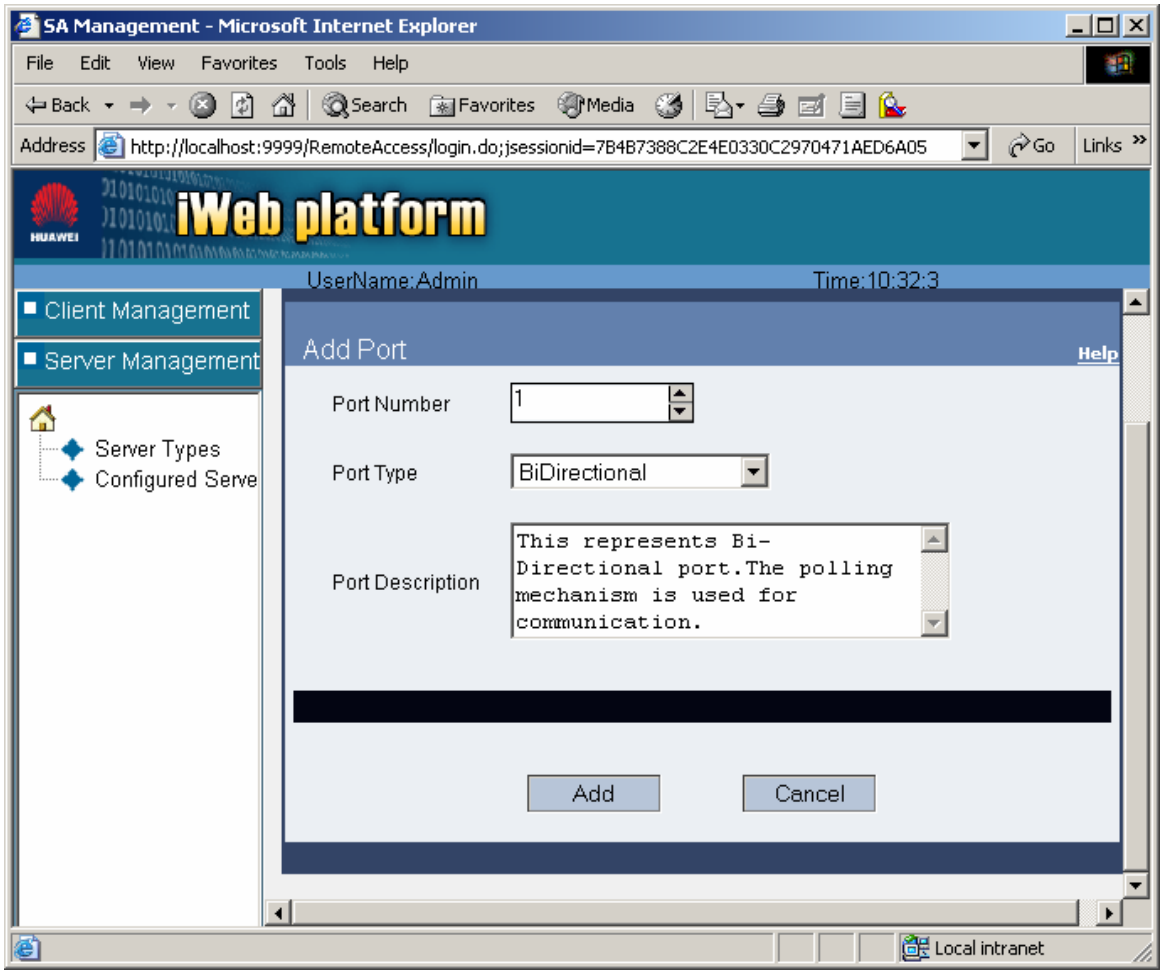


Figure 3-16 “Add Port” window

Fill in various port parameters based on actual needs. Click <Add> to add the port attribute of the server.

4) Then return to the interface as shown in Figure 3-15. Click <Add> and add a new server type in the window “View Server Types”, as shown in Figure 3-17.

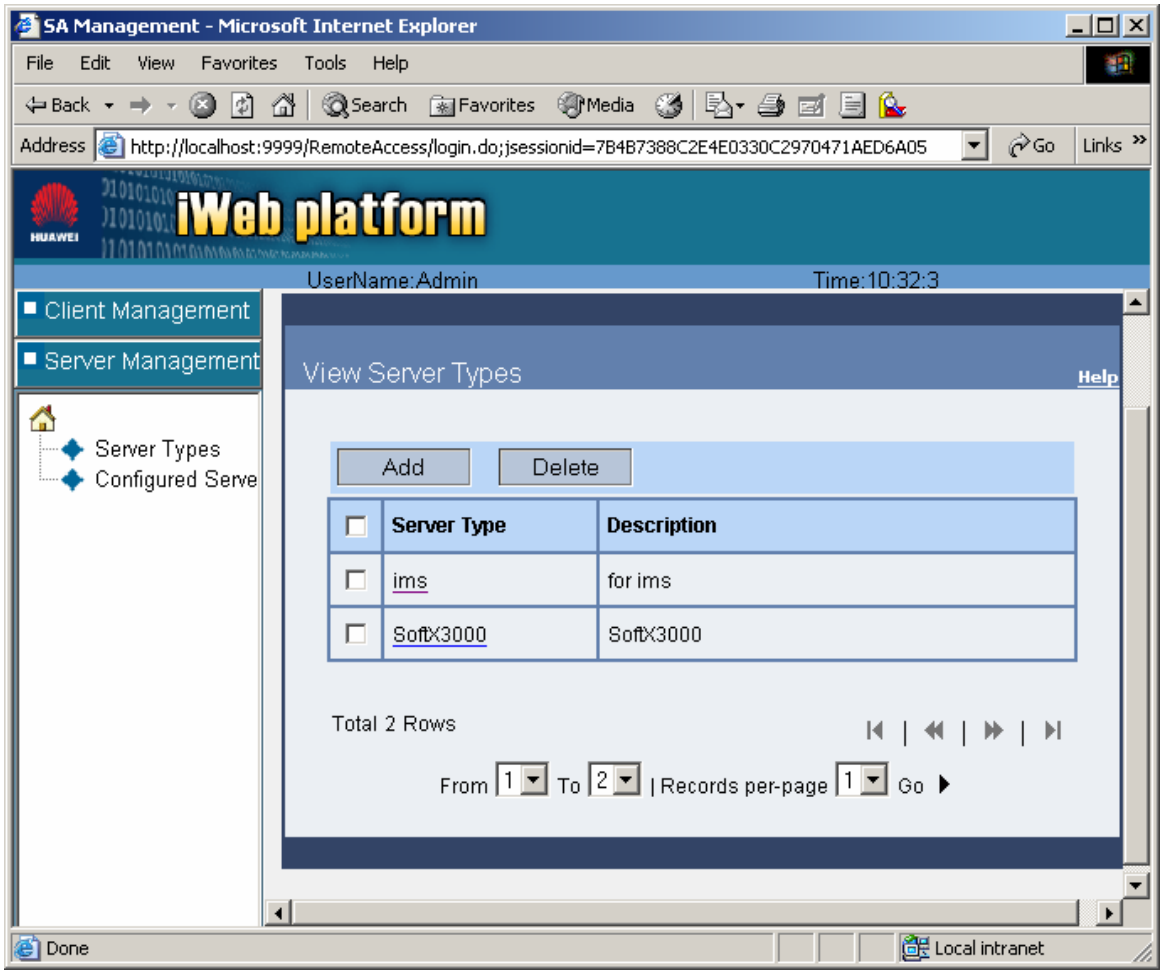


Figure 3-17 Upgraded server type

II. Deleting Server Types

In the window “View Server Types” as shown in Figure 3-14, select a server type to be deleted; that is, tick off a server type. Click <Delete>.

3.3.6 Configuring Server Instances

Configuring server instances means configuring servers to be maintained. It includes adding server instances, deleting server instances, and refreshing server statuses.

I. Adding Server Instances

1) In Figure 3-14, click the submenu “Configured Server” under the left navigation menu. The window “View Configured Server List” is displayed on the right, as shown in Figure 3-18.

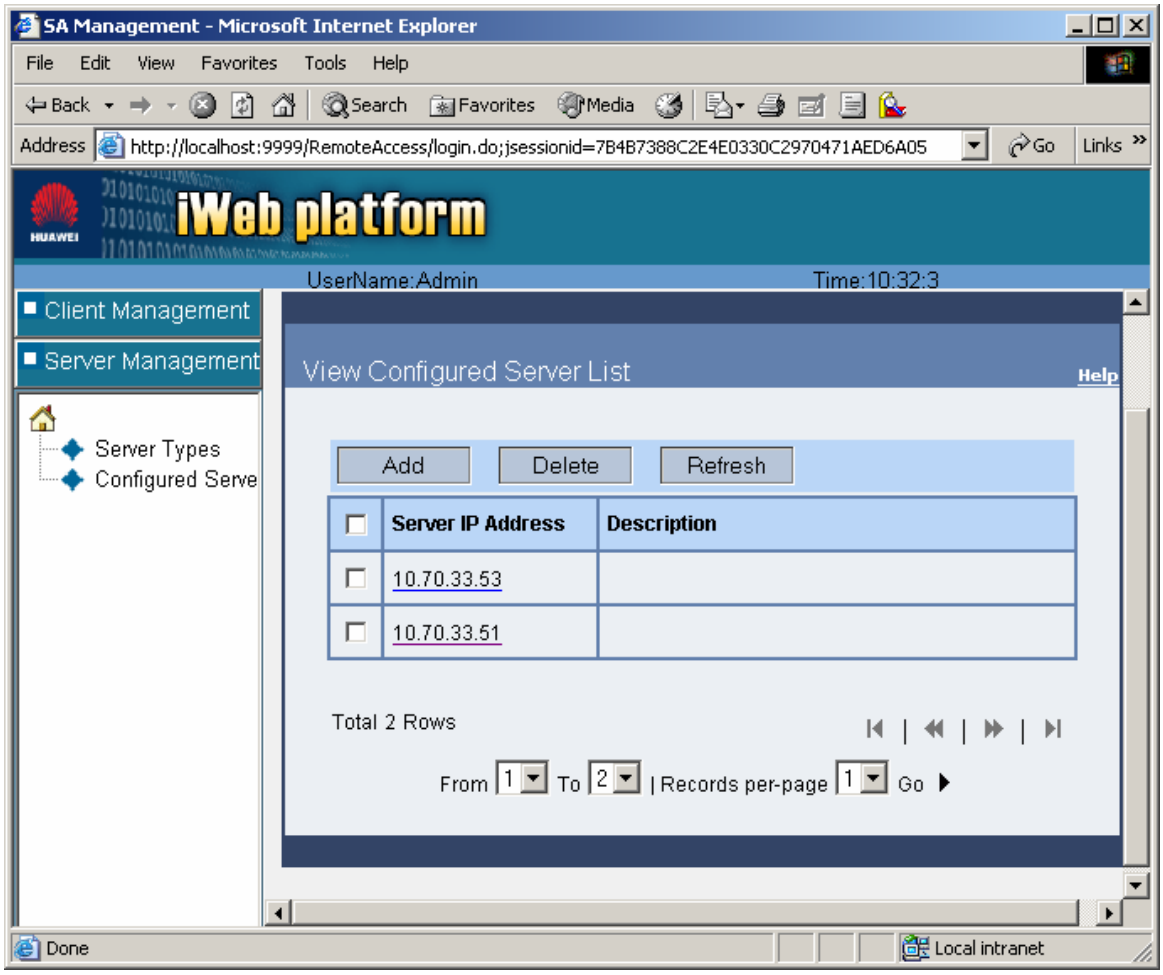


Figure 3-18 “View Configured Server List” window

2) Click <Add>. The window “Add Server Information” is displayed on the right of the interface, as shown in Figure 3-19.

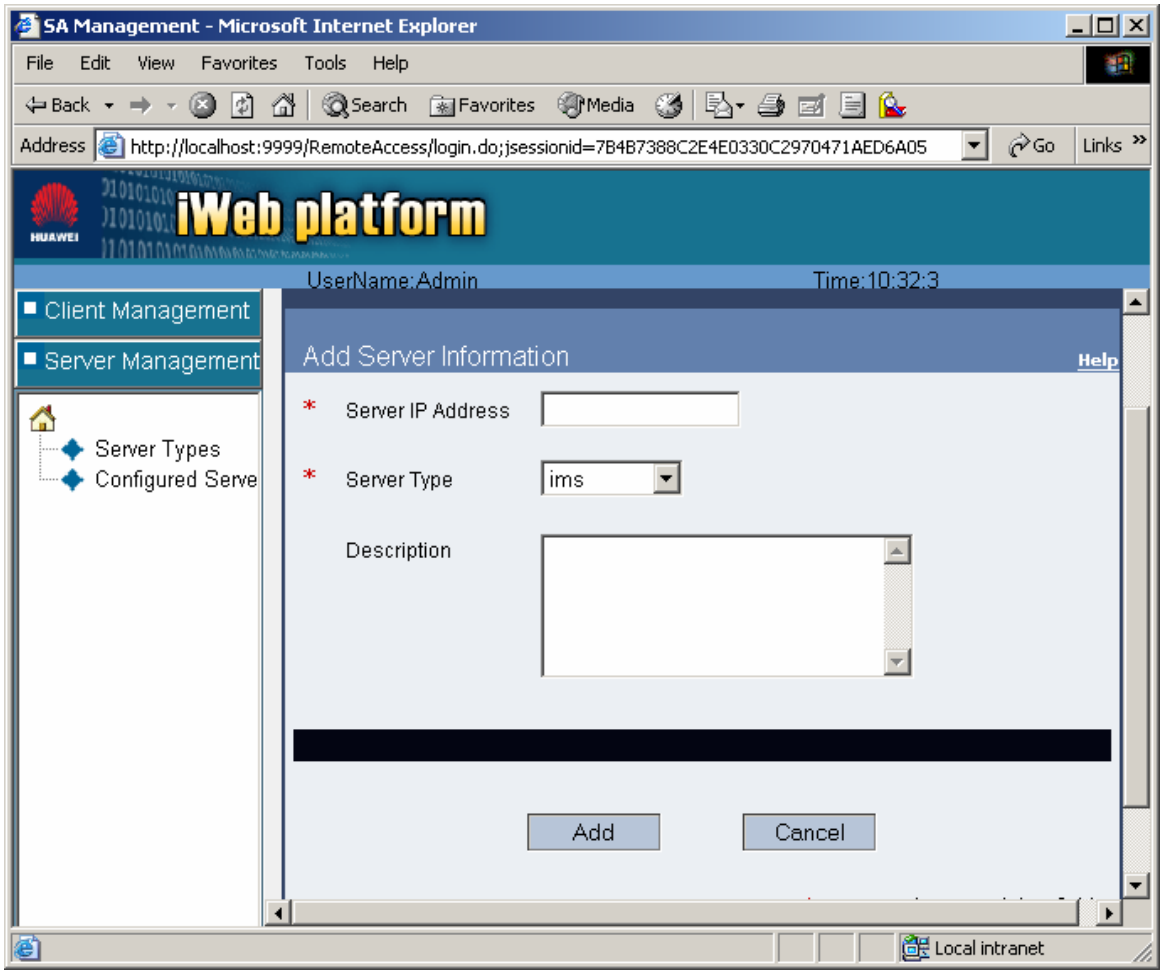


Figure 3-19 “Add Server Information” window

3) Enter the server IP address, server type, and related description. Click <Add>, and then a new server instance is added in the window “View Configured Server List”, as shown in Figure 3-20. For configuring server types, refer to “3.2.5 Configuring Server Types”.

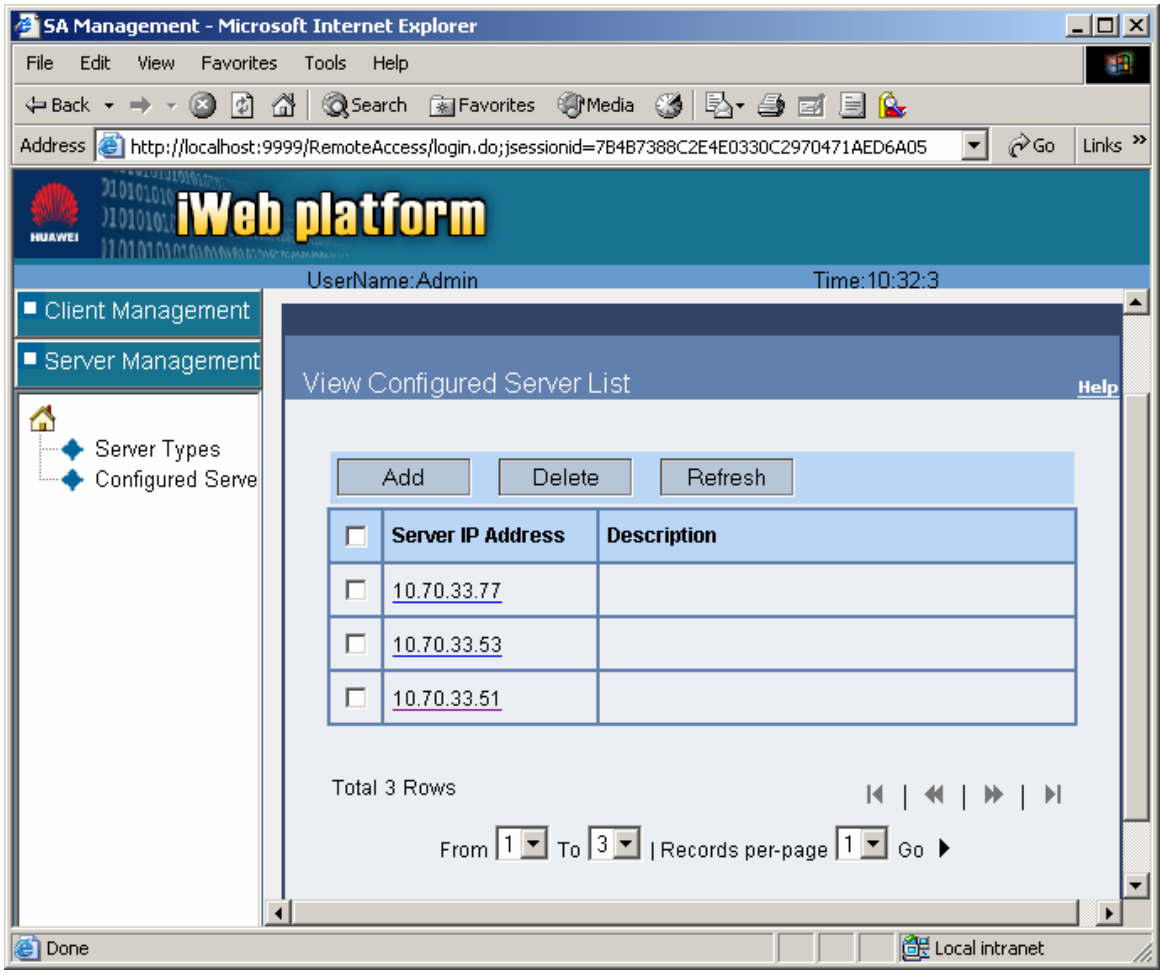


Figure 3-20 Upgraded server list

II. Deleting Server Instances

Proceed as follows:

1) In the window “View Configured Server List” as shown in Figure 3-18, select a server to be deleted; that is, tick the checkbox before the server type. Click <Delete>. A prompt is displayed, as shown in Figure 3-21.

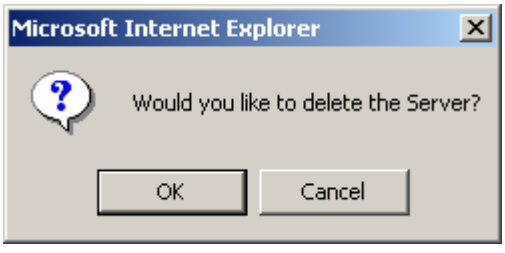


Figure 3-21 Prompt information of deleting a server

2) Click<OK>.

III. Refreshing Server Statuses

In the window “View Configured Server List” as shown in Figure 3-18, click <Refresh> to check the latest server instance configuration.

3.4 RAC Data Configuration

The RAC data configuration includes:

- Configuring system attribute file
- Configuring log functions
- Configuring proxy information
- Configuring maintenance terminal access strategy

3.4.1 Configuring the System Attribute File

The system attribute file **system.properties** includes such options as language of RAC, country and lookandfeel. The following describes the configuration steps:

1) Enter the RAS installation directory. The default is C:\Remote Access\Client.
2) Use the text editor to open the file **lsystem.properties** under the directory conf. Table 3-3 shows the meanings of various configuration items. You can modify various configuration items based on actual needs.

Table 3-3 Configuration item description

Configuration item	Description
language	Language option. en means English; zh means Chinese; the default value is en.
country	Country option. US means America; CN means Chinese; the default value is US.
lookandfeel	It includes Motif, Metal, Huawei and Windows. The default value is Metal.
maxconnections	Maximum number of connected maintenance terminals. The default value is 10; that is, at most 10 maintenance terminals can be connected. It is recommended not to modify the default value.

The following shows the typical system attribute configuration.

```
language=en
country=US
#lookandfeel=Motif
lookandfeel=Metal
#lookandfeel=Huawei
#lookandfeel=Windows
maxconnections=10
```

Note:

Upon selecting the lookandfeel option, you only need to delete "#" before the lookandfeel option to enable it. Note that only one lookandfeel option can be enabled at any time. It is recommended to adopt the default value.

3.4.2 Configuring Log Functions

The RAC log function configuration is the same as that of the RAS. It includes the file name **logconfig.xml**, the relative path of the configuration file, and meanings and value ranges of various configuration items. The difference is that the default directory of the RAC is C:\Remote Access\Client. For configuring the RAC log functions, refer to "3.2.3 Configuring Log Functions".<0}

3.4.3 Configuring Proxy Information

1) The RAC accesses Internet through a proxy server, as shown in Figure 1-1. Before using an RAC, you must set proxy information. Specific steps: Select [Start/Programs/Remote Access/ Remote Access Client] in a computer installed with the RAC software to display the RAC login window, as shown in Figure 3-22.

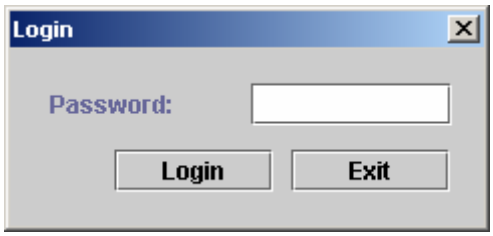


Figure 3-22 RAC login window

2) Enter the correct login password which has been set when installing the RAC software. Click <Login> to enter the RAC service interface, as shown in Figure 3-23.

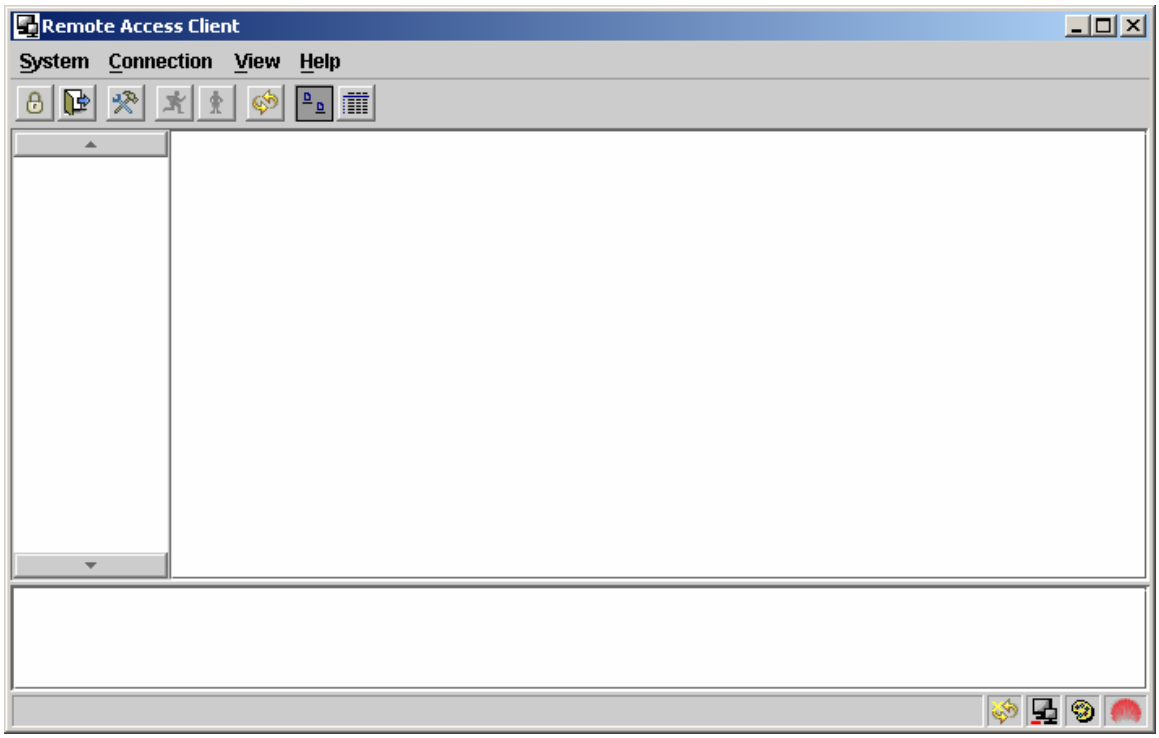


Figure 3-23 RAC service interface

3) Select [System/Settings], or click on the tool bar. The window "Setting" is displayed, as shown in Figure 3-24.

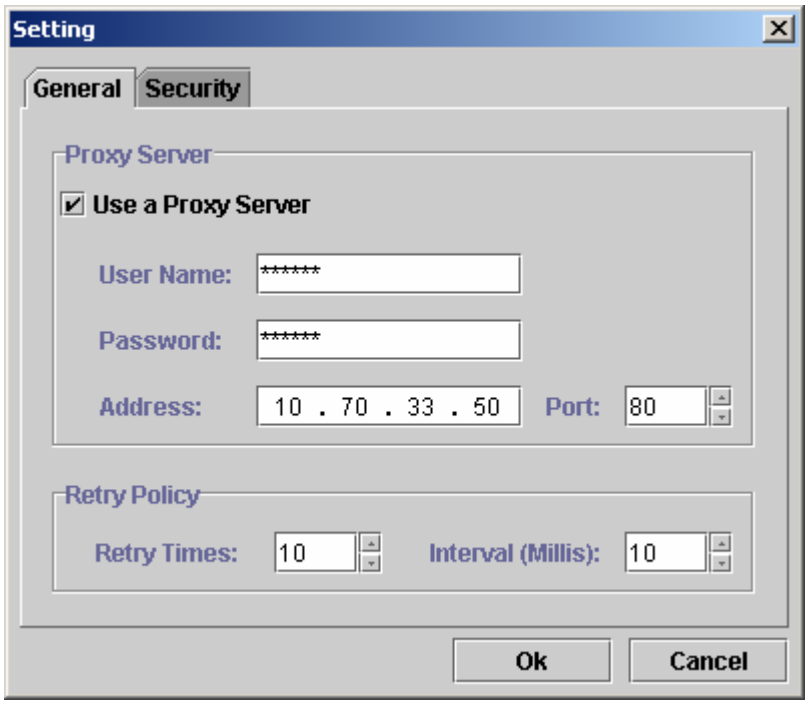


Figure 3-24 "Setting" window

4) In the tab “General”, tick the checkbox before the “Use a Proxy Server”, enter the user name, password, IP address and ports, and set retry times and retry time interval. Click <OK>.

Note:

- Retry times mean the total retry connection times when the RAC fails to connect a proxy server. The default value is 10.
- Retry time interval means the time interval between two retries. The default value is 10 minutes. It is recommended to adopt the default value.
- The port number here means the port number of the proxy server, not the port number of HTTP or HTTPS.

3.4.4 Configuring Maintenance Terminal Access Strategy

The maintenance terminal access strategy means to add or remove an IP address range of maintenance terminals that can or cannot access the RAC so as to ensure the security of the remote maintenance access system. The following describes the specific steps.

1) Log in the RAC service interface, as shown in Figure 3-23.
2) Select [System/Settings], or click on the tool bar. The window “Setting” is displayed, as shown in Figure 3-24.
3) In the window "Setting” , click the tab “Security”, as shown in Figure 3-25.

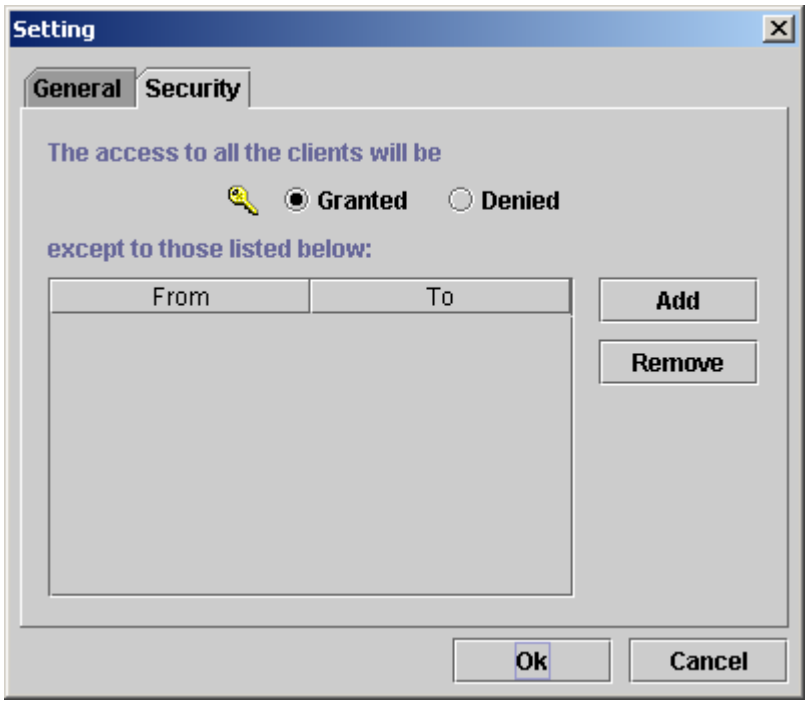


Figure 3-25 Tab “Security”

4) Select an IP address range of maintenance terminals to be added or removed.

- If you need to add IP address ranges of maintenance terminals that can access the RAC, select “Granted” and click <Add>. The dialog box “Add IP Range” is displayed, as shown in Figure 3-26.

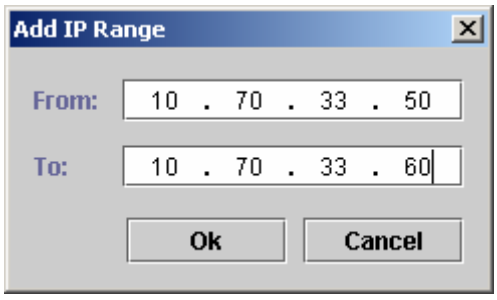


Figure 3-26 “Add IP Range” dialog box

5) Enter an IP address range, and click <OK>. The above IP address range is added, as shown in Figure 3-27.

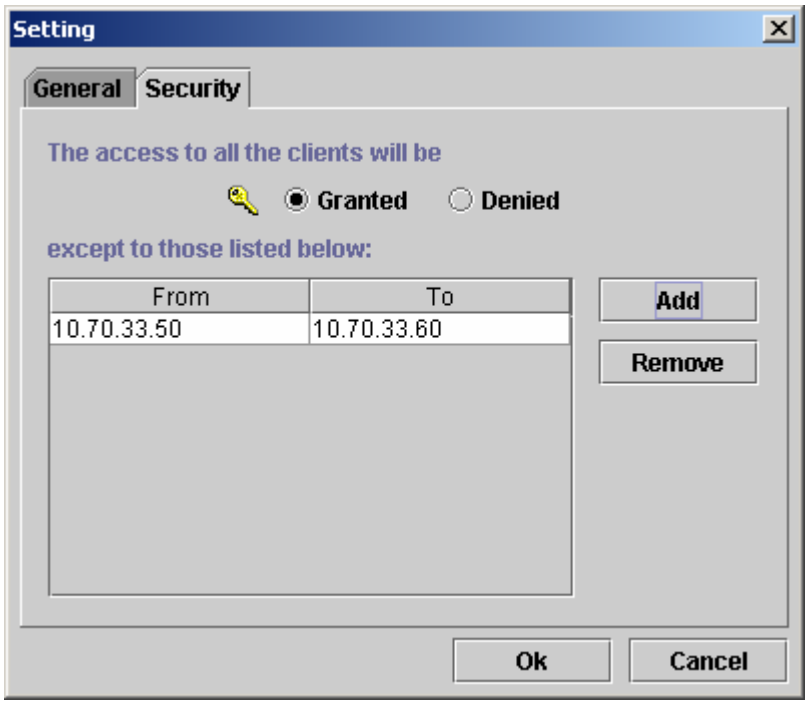


Figure 3-27 Add maintenance terminals that can access to RAC

- If you need to add an IP address range of maintenance terminals that cannot access the RAC, select “Denied” and click <Add>. The dialog box “Add IP Range” is displayed, as shown inFigure 2-26.

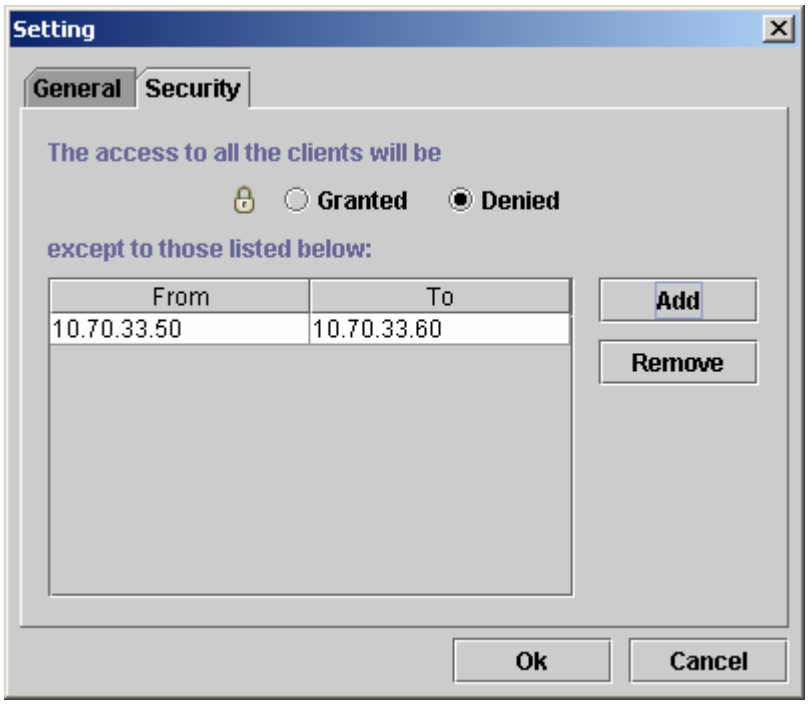


Figure 3-28 Add maintenance terminals that cannot access RAC

Enter an IP address range, and click <OK>. The above IP address range is added, as shown in Figure 3-28.

- If you need to remove an IP address range of maintenance terminals that can access the RAC, select “Granted”. Then select an IP range to be deleted from the IP address list and click <Remove>.
- If you need to remove an IP address range of maintenance terminals that cannot access the RAC, select “Denied”. Then select an IP range to be deleted from the IP address list and click <Remove>.

Note:

- If the IP address ranges of maintenance terminals that can access the RAC and the IP address ranges of maintenance terminals that cannot access the RAC overlap, the latter has a priority; that is, the corresponding maintenance terminals are denied to access the RAC.
- If you do not add the IP address of a maintenance terminal in the IP address ranges of maintenance terminals that can access the RAC and the IP address ranges of maintenance terminals that cannot access the RAC, the maintenance terminal are denied to access the RAC by default.

3.5 RAS Basic Operation

3.5.1 Starting RAS Background Service

1) Select [Start/Programs/Remote Access/Start Remote Access Server] or run the file **run.bat** under the installation directory of the RAS. A window is displayed, as shown in Figure 3-29. By now, the RAS background service is started. If you have configured the RAS data and the RAC data and the connection request from an RAC has passed the RAS authentication, you can start remote maintenance.

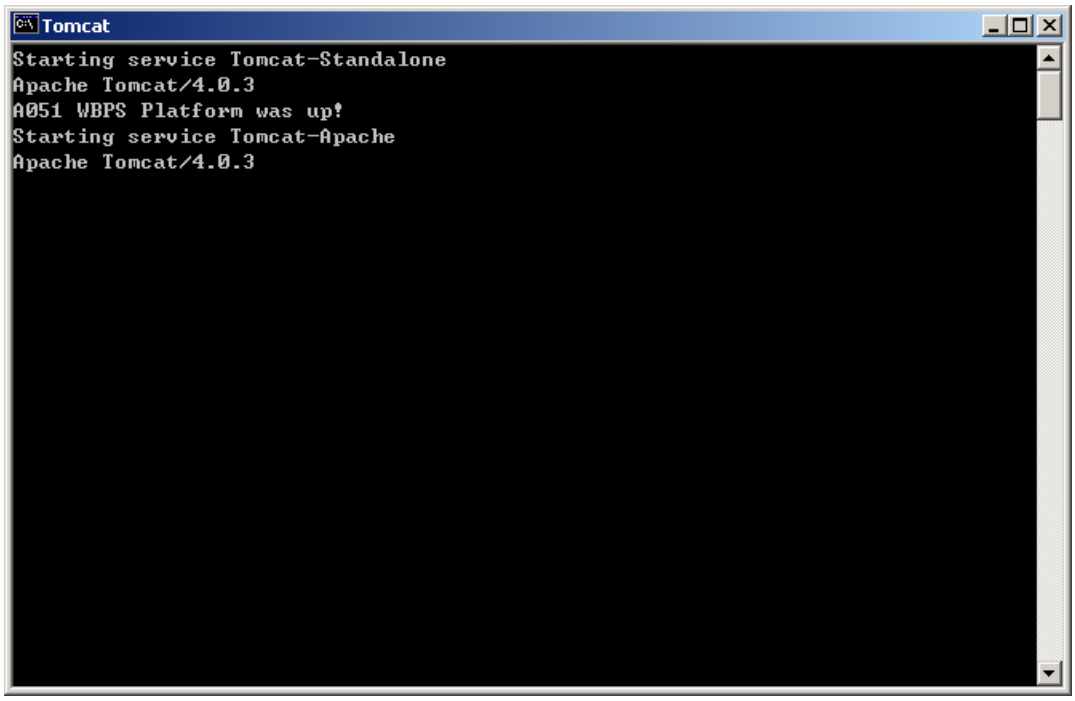


Figure 3-29 RAS service start window

3.5.2 Logging in RAS Service Interface

For details, refer to “3.2.4 Configuring Connection Instances”.

3.5.3 Reviewing Connection Requests Manually

When the RAC sends a connection request to the RAS, the system approves the request automatically and establishes a connection if the connection instance has been configured on the RAS. If the connection instance is not configured on the RAS, you need to check the connection request manually. The following describes the specific steps.

1) Log in the RAS service interface
2) In the RAS service interface shown in Figure 3-1, click the menu item “Client Management” under the left navigation menu, and then click the submenu “Waiting Authorize”. The window “Client Agents Waiting Authorization” appears in the right window, as shown in Figure 3-30.

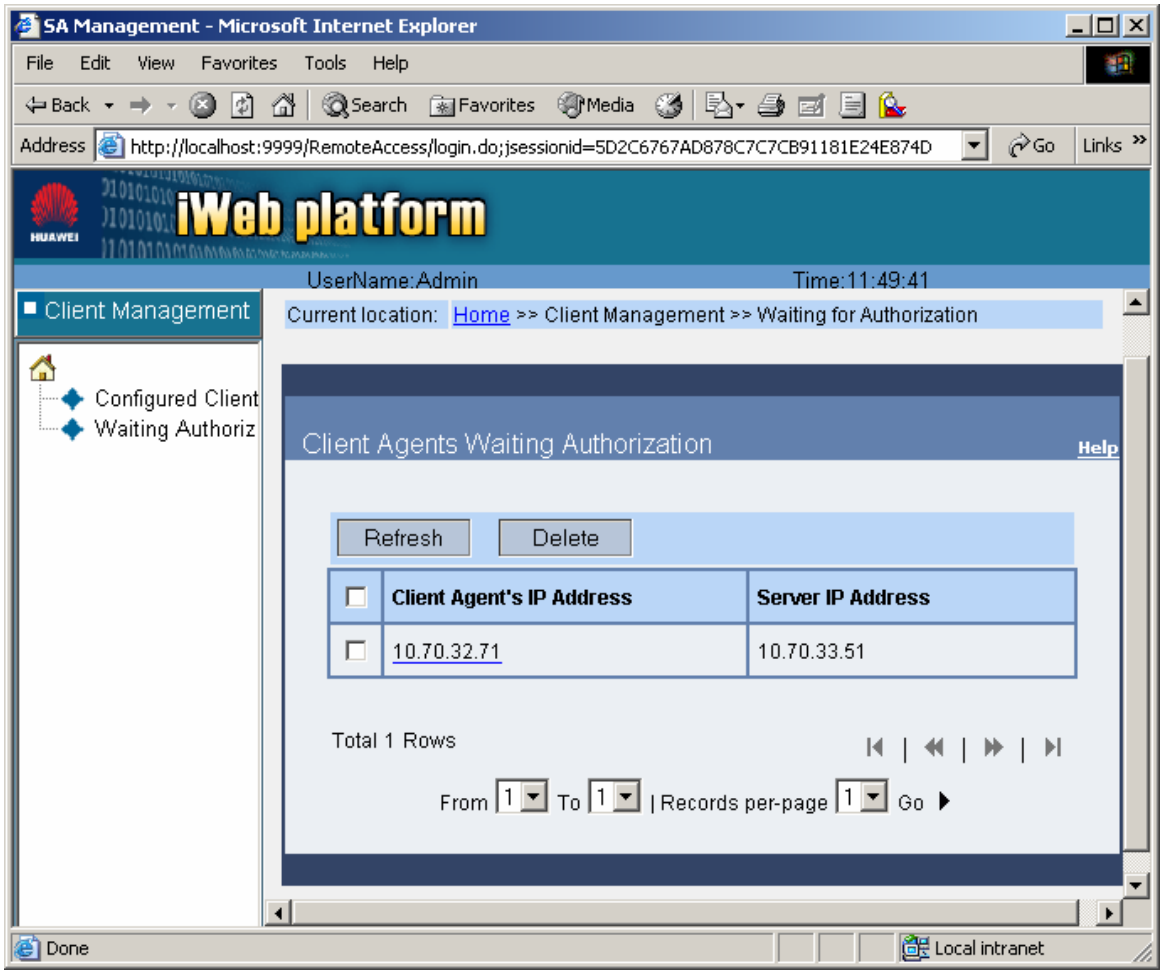


Figure 3-30 “Client Agents Waiting Authorization” window

3) Review whether to accept the connection request based on actual needs. If not, select the request and click <Delete>. If yes, click the IP address of the RAC directly. Then the window “Add Client Session Information” is displayed, as shown in Figure 3-31.

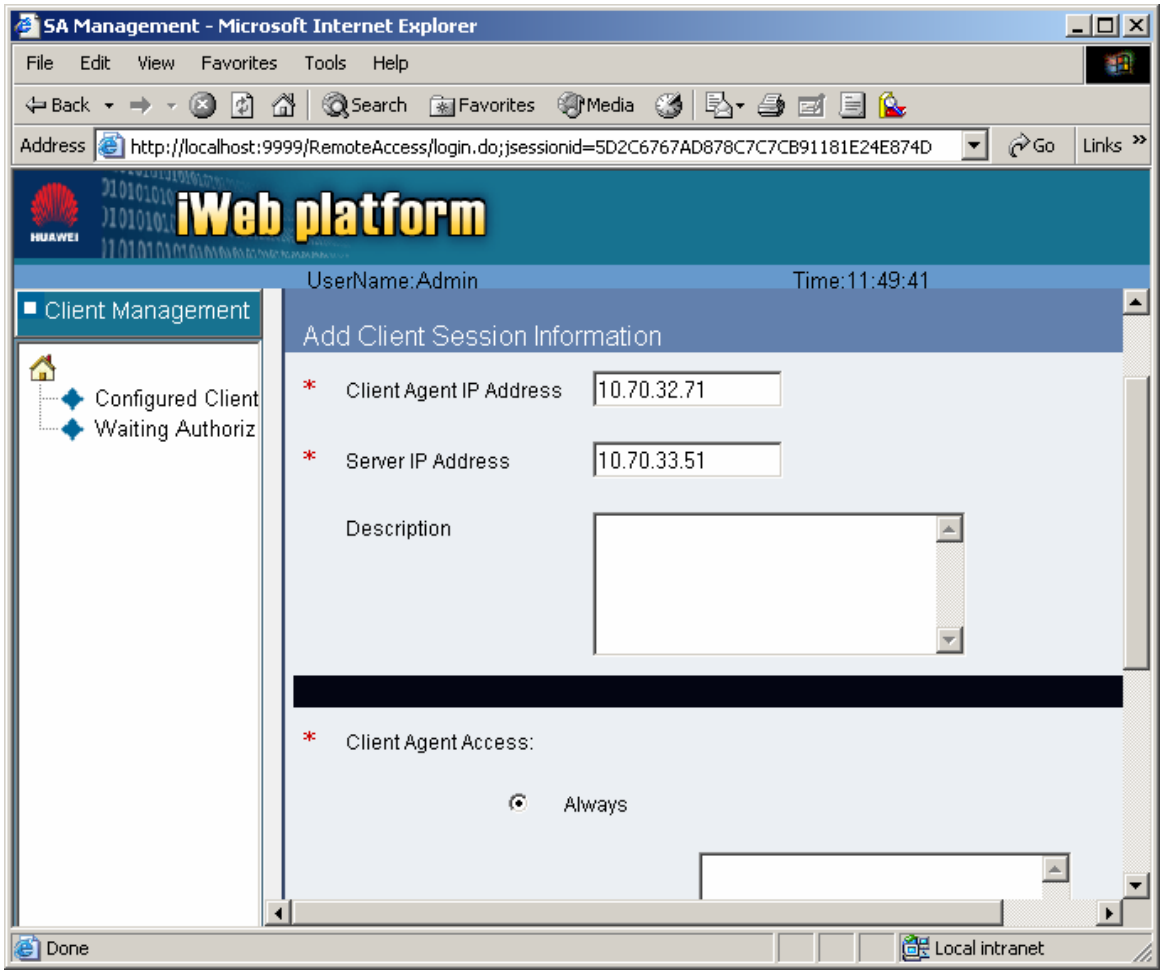


Figure 3-31 “Add Client Session Information” window

4) Refer to “3.2.4 Configuring Connection Instances” to add the “RAC” to the “Client Session List”. The corresponding connection request disappears from the window “Client Agents Waiting Authorization” after the connection instance is added; that is, the connection request has been accepted.

3.5.4 Changing RAS Login Password

The following describes the specific steps:

1) Log in the RAS service interface
2) In the RAS service interface shown in Figure 3-1, click the menu item “Configure SA Admin” under the navigation menu and then click the submenu “Change Password". The window “Change SA Admin password” is displayed on the right, as shown in Figure 3-32.

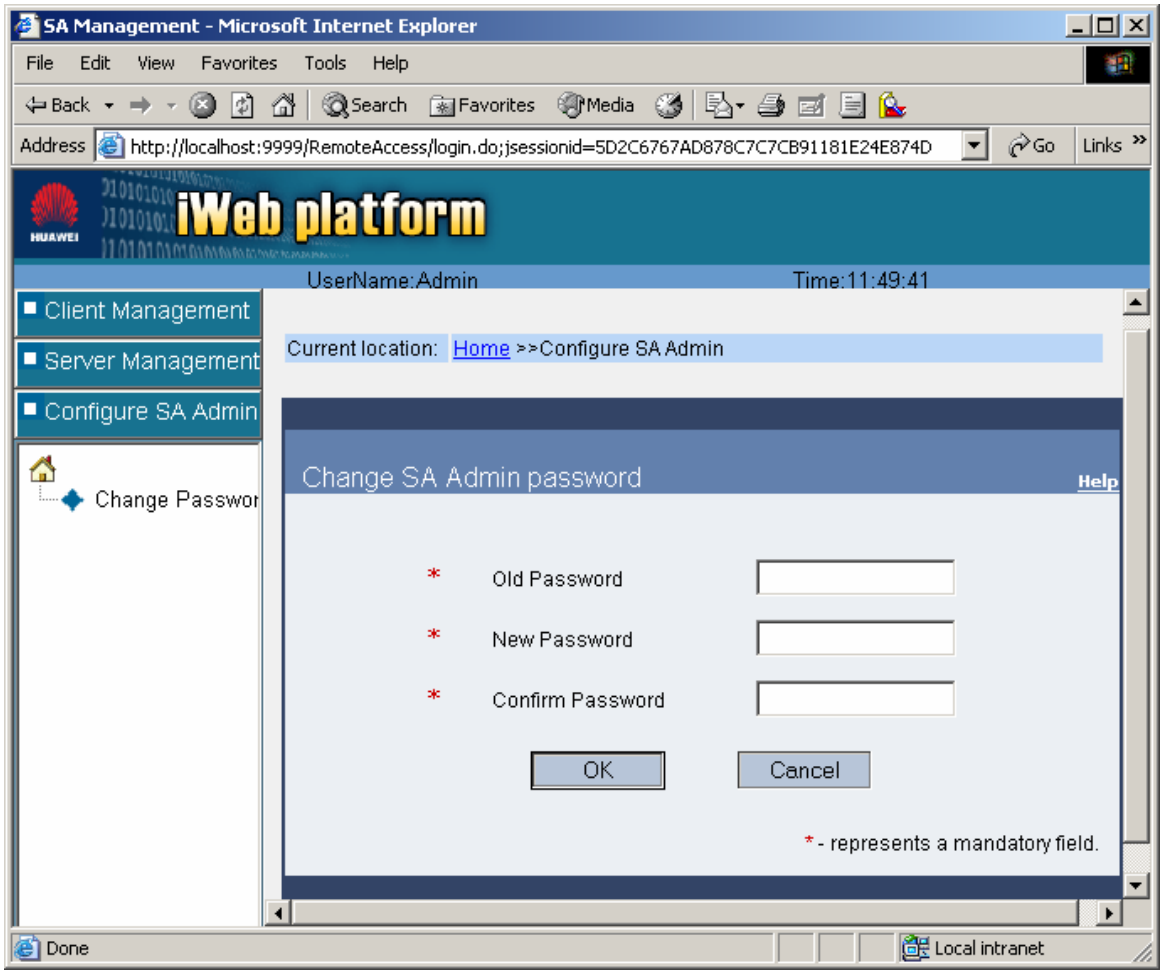


Figure 3-32 “Change SA Admin password” window

3) Enter old password, new password, confirm password, and then click <OK>. A prompt “Password Changed Successfully” is displayed on the right of the interface, as shown in Figure 3-33.

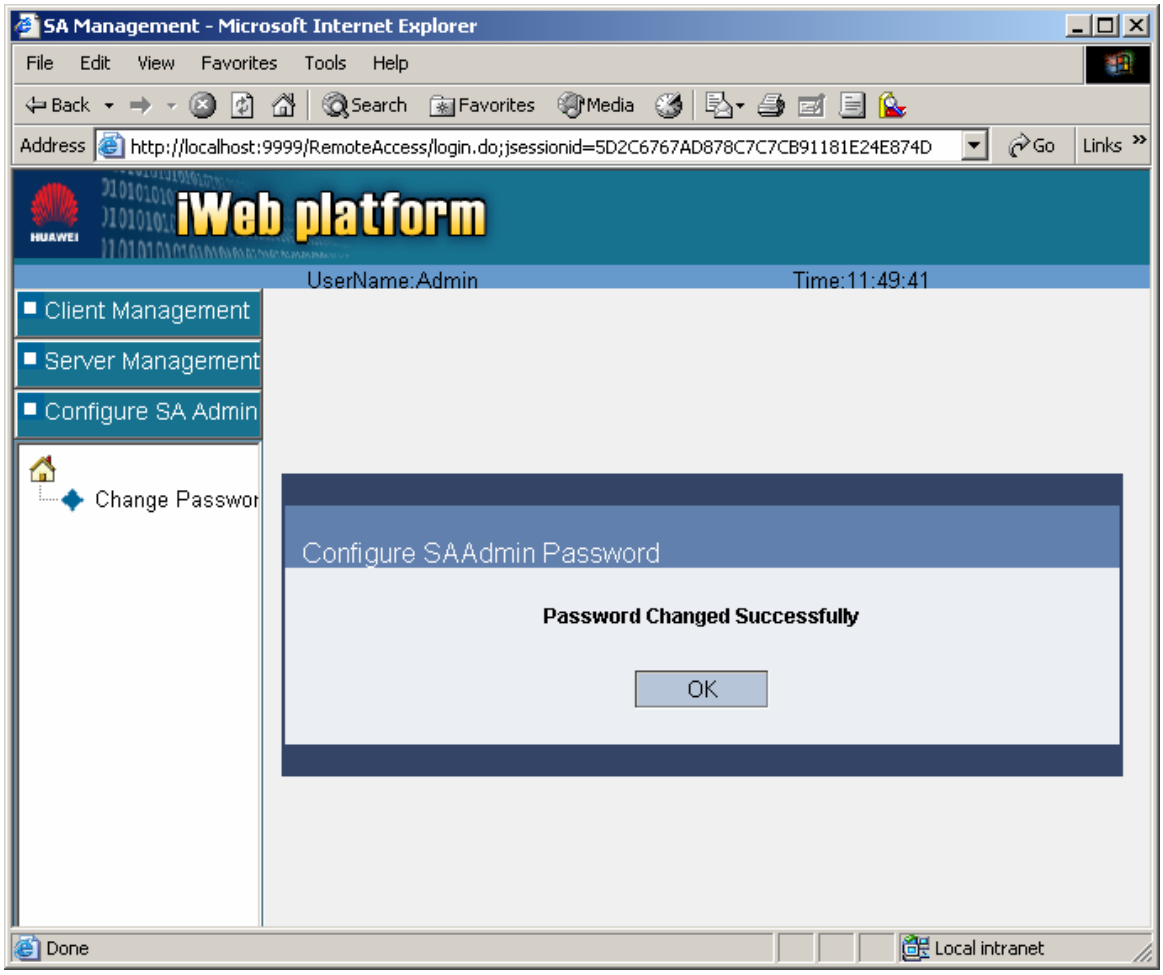


Figure 3-33 “Password Changed Successfully” prompt information

(4) Click <OK>.

3.5.5 Logging Out RAS

The following describes the specific steps:

1) In the RAS service interface (as shown in Figure 3-1), click the menu item “Logout” under the navigation menu on the left. The window “Logout Server Agent” is displayed on the right, as shown in Figure 3-34.

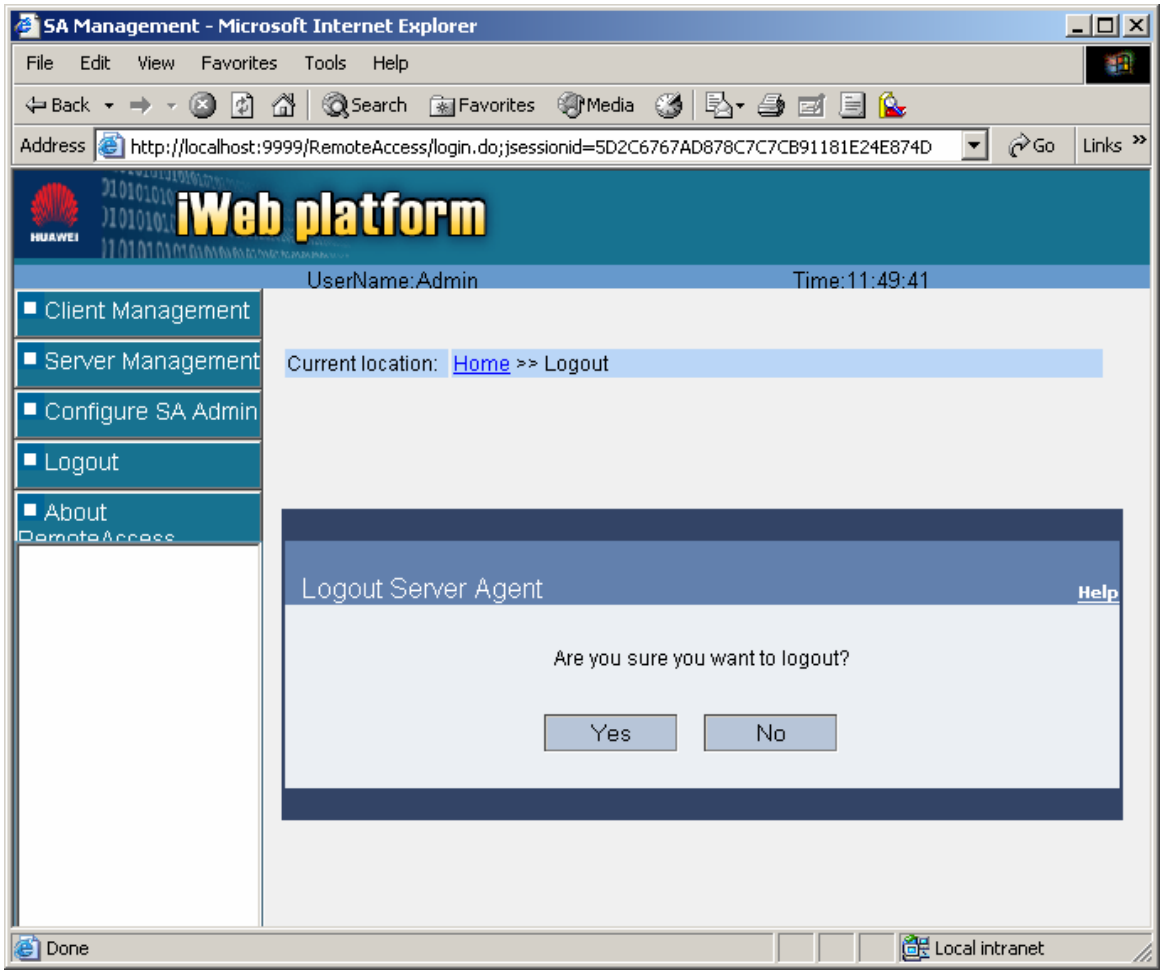


Figure 3-34 “Logout Server Agent” window

2) Click <Yes>.

3.5.6 Showing Online Help

The following describes the specific steps:

1) In the RAS service interface (as shown in Figure 3-1), click the menu item “About RemoteAccess” under the navigation menu on the left. The help home page is displayed in the right window, as shown in Figure 3-35.

SA Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:9999/RemoteAccess/login.do;jsessionid=5D2C6767AD878C7C7CB91181E24E874D
Go Links
iWeb platform
UserName:Admin
Time:11:49:41
Client Management
Server Management
Configure SA Admin
Logout
About
Show
About iWeb Remote Access
iWeb Remote Access is a platform that facilitates remote maintenance over Internet through firewalls and proxies. In a normal scenario, if the Client is not on Server's local network, then it cannot connect to the server. The reason is the client-server protocol is not being supported by proxies, whereas the iWeb Remote Access provides a platform, using which the remote maintenance can be done despite the presence of firewalls and proxies.
The two major components in iWeb Remote Access platform are:
Remote Access Client (RAC) – The component of RAC, that has been installed on the remote user machine acts as a proxy server for the actual server application.
Remote Access Server (RAS) – The proxy on the server network, which maintains the connection with the server application.
Done
Local intranet

Figure 3-35 Help home page

2) In the above figure, click “Show” in the right page. A complete online help page is displayed in the right window, as shown in Figure 3-36.

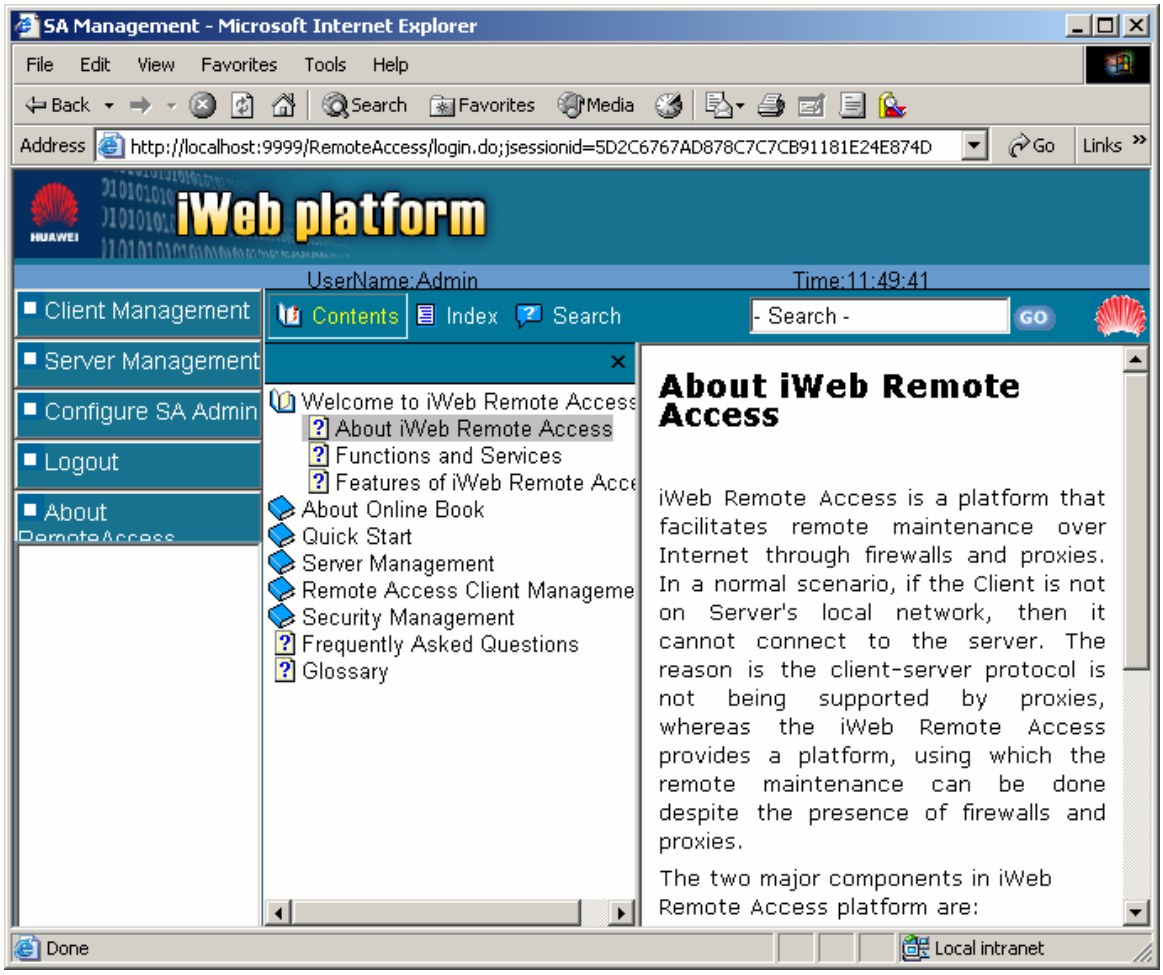

SA Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost:9999/RemoteAccess/login.do;jsessionid=5D2C6767AD878C7C7CB91181E24E874D
Go Links
iWeb platform
UserName:Admin
Time:11:49:41
Client Management
Server Management
Configure SA Admin
Logout
About
Contents Index Search
- Search -
GO
Welcome to iWeb Remote Access
About iWeb Remote Access
Functions and Services
Features of iWeb Remote Acce
About Online Book
Quick Start
Server Management
Remote Access Client Manageme
Security Management
Frequently Asked Questions
Glossary
About iWeb Remote Access
iWeb Remote Access is a platform that facilitates remote maintenance over Internet through firewalls and proxies. In a normal scenario, if the Client is not on Server's local network, then it cannot connect to the server. The reason is the client-server protocol is not being supported by proxies, whereas the iWeb Remote Access provides a platform, using which the remote maintenance can be done despite the presence of firewalls and proxies.
The two major components in iWeb Remote Access platform are:
Done
Local intranet

Figure 3-36 Online help window

Also, you can click <Help> to open help files.

3.5.7 Closing RAS Background Service

Select [Start/Programs/Remote Access/Stop Remote Access Server] in the computer installed with the RAS software, then the window shown in Figure 3-29 and the RAS background service close.

3.6 RAC Basic Operation

3.6.1 Logging in RAC Service Interface

For details, refer to "3.3.3 Configuring Proxy Information".

3.6.2 Changing RAC Login Password

In the RAC service interface, select [System/Change Password]. The window “Change Password” is displayed, as shown in Figure 3-37.

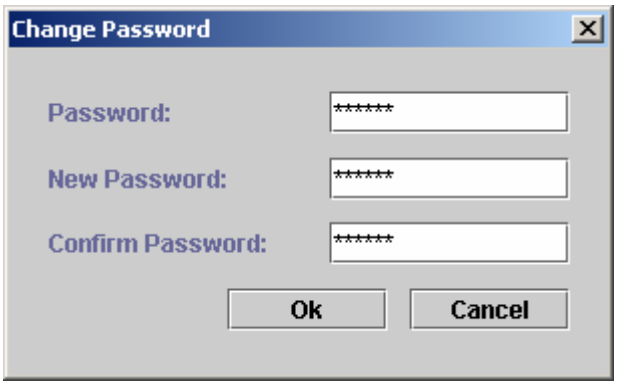


Figure 3-37 "Change Password" window

Enter the old password and a new one, and then confirm the new password. Click <OK>.

3.6.3 Locking and Unlocking

In the RAC service interface, select [System/Lock] or click the icon on the tool bar directly. Then the system enters the locking status and the window "Unlock" is displayed, as shown in Figure 3-38.

Figure 3-38 "Unlock" window

The system can be unlocked only when you enter the correct login password.

3.6.4 Establishing/ Deleting a Connection to RAS

I. Establishing a Connection to the RAS

The following describes the specific steps:

1) In the RAC service interface, select [Connection/New]. The window "New Connection" is displayed, as shown in Figure 3-39.

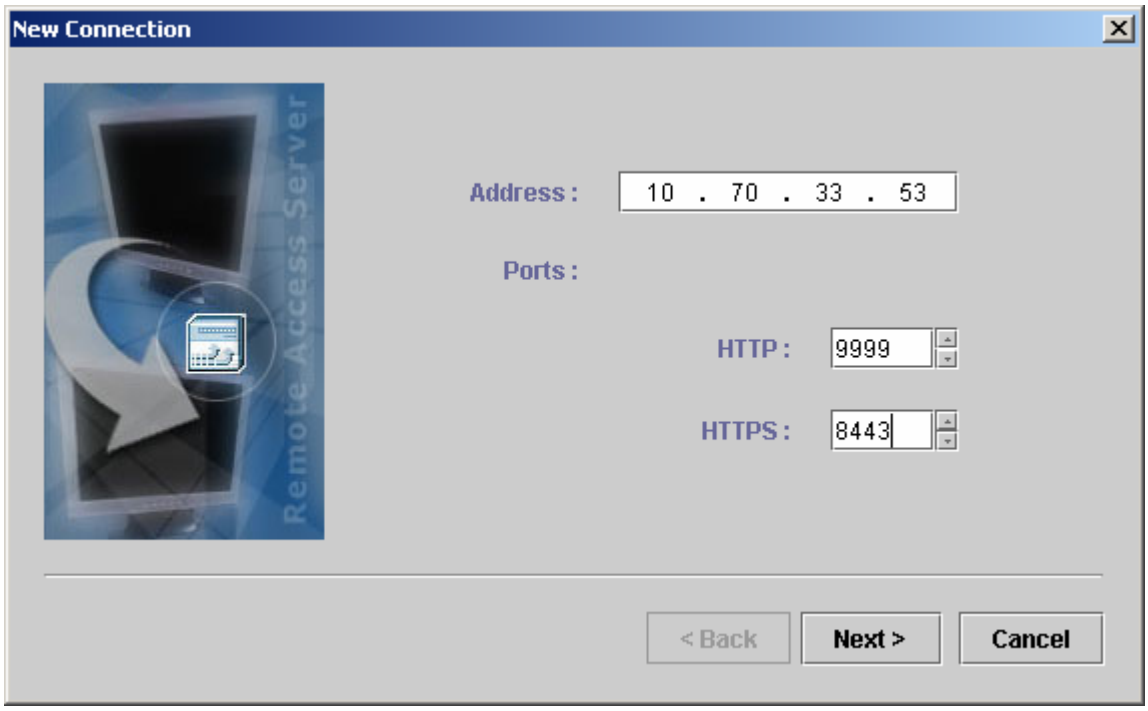


Figure 3-39 "New Connection" window

In the above figure,

- Enter the IP address of the RAS in the "Address" box.
- Enter port numbers of HTTP and HTTPS in the "Ports" box. The entered port numbers must be consistent with those of HTTP and HTTPS set on the RAS. For details about port number setting on the RAS, refer to "3.2.1 Configuring IP Address and Ports". By default, the port number of HTTP is 9999 and that of HTTPS is 8443.<0}

2) Click <Next>. The window "Select Equipment Server" is displayed, as shown in Figure 3-40.

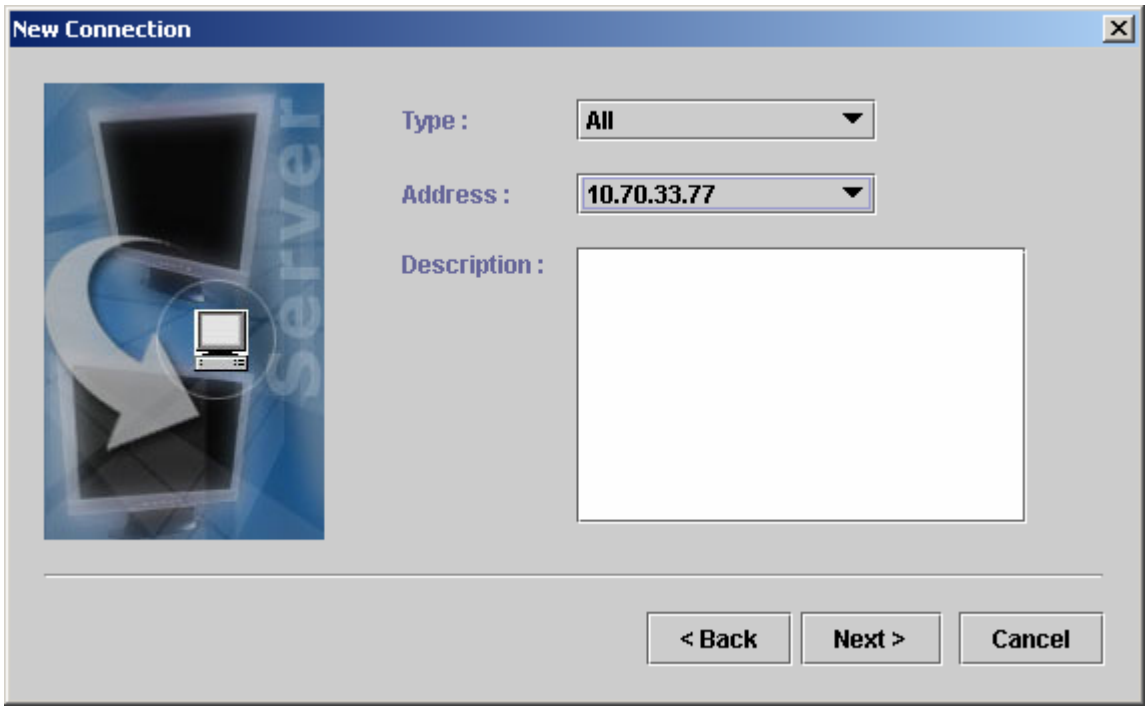


Figure 3-40 "Select Equipment Server" window

3) Select the type and IP address of the server to be maintained,, and enter related description. Click <OK>. The window "Port Setting" is displayed, as shown in Figure 3-41.

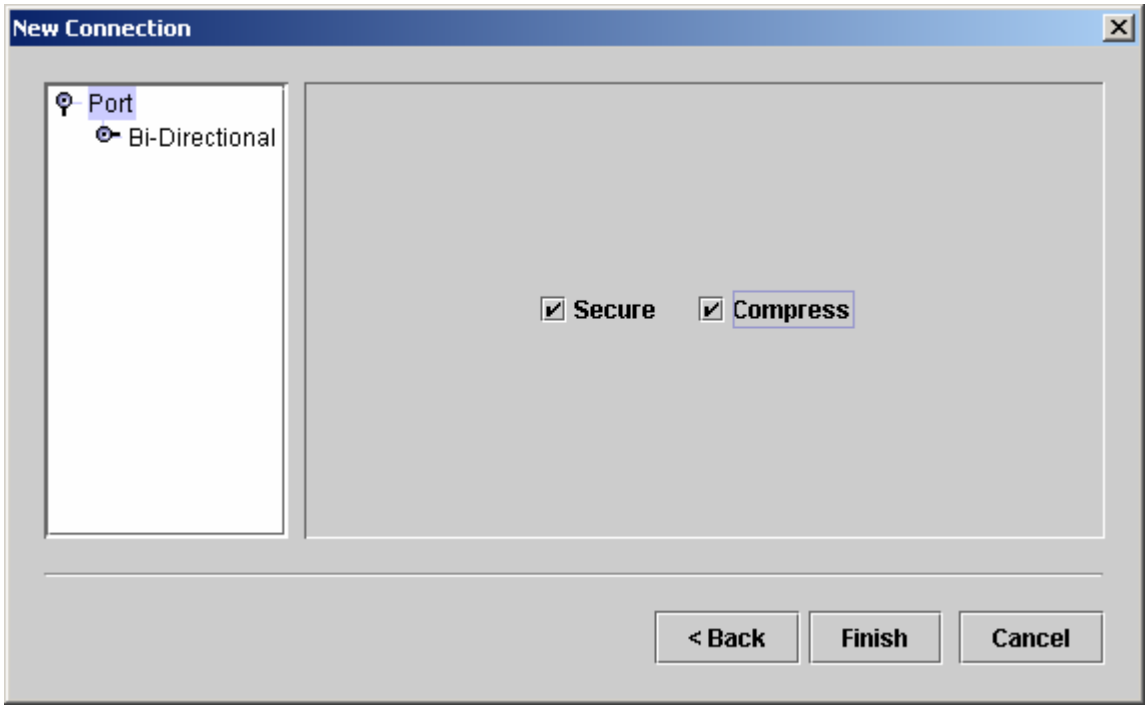


Figure 3-41 "Port Setting" window

In the above figure,

- Secure: It provides the encryption function.
- Compress: It provides the compression function to help use network bandwidth more effectively.

Select whether to encrypt and compress port data based on actual needs. If necessary, tick the checkbox before the corresponding option. By default, both are not ticked. If both are selected, the corresponding options of bi-directional port and reporting port will be ticked.

4) Click the node “Bi-Directional” under the right navigation tree in the window “Port Setting”. The window “Set Bi-Directional Port” is displayed, as shown in Figure 3-42.

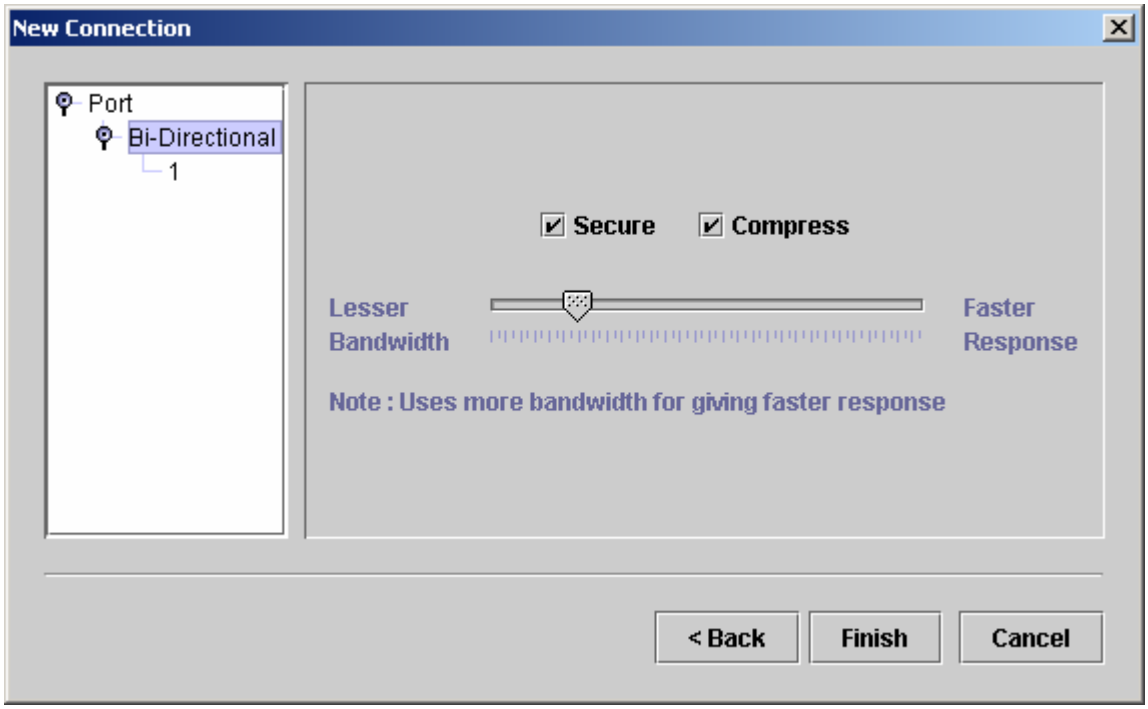


Figure 3-42 “Set Bi-Directional Port” window

In the above figure,

Performance: By this selection, you can select lesser bandwidth to get higher performance. The RAC uses the polling mechanism to obtain the RAS response. If you select lesser bandwidth, the polling time interval will be longer

5) Click <Finish>. At this time, the RAC sends a connection request to the RAS.

- If the connection request is passed, a new server icon appears in the RAC service interface. The icon color is sky blue, as shown in Figure 3-43. The status bar in the lower part displays connection information, including proxy IP address, IP address of the RAS, and the connection request status. Proxy server: 10.70.33.53; server: 10.70.33.77; status: Authorized.

Note:

In the RAC service interface, the RAS icons are displayed in the left window; the icons of servers to be maintained are displayed in the right window. IP addresses are displayed below the server icons. The RAS icons correspond to those of servers in the right window.

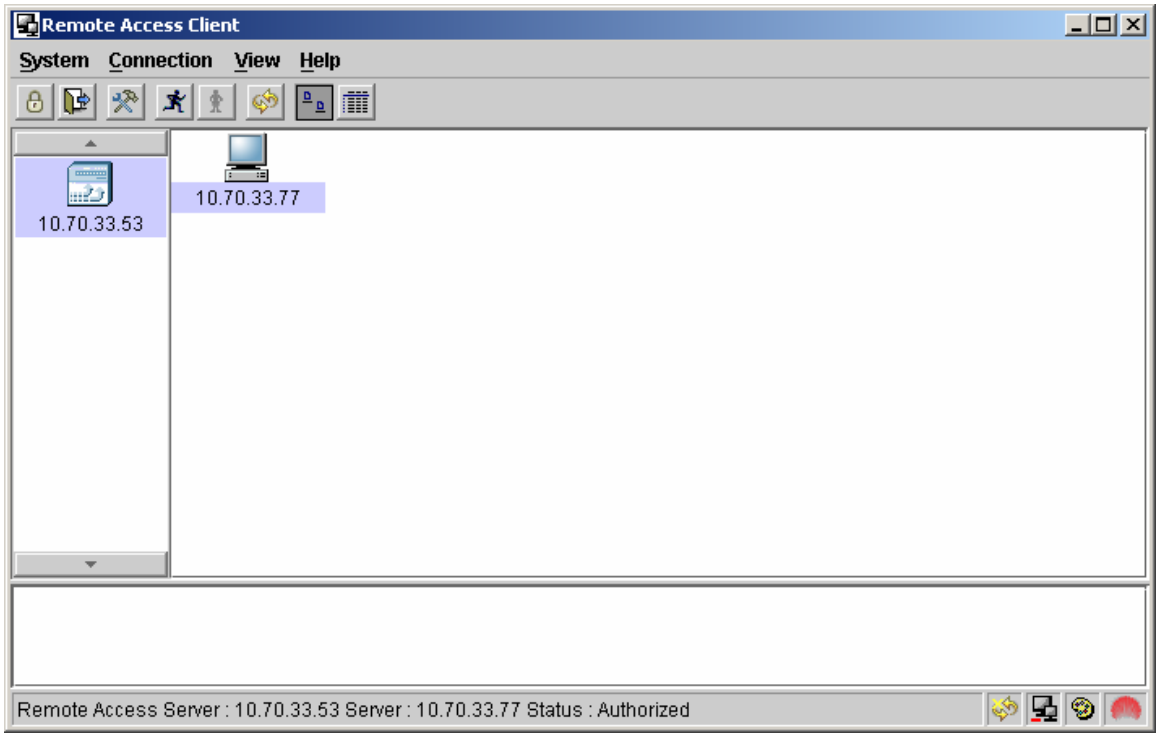

Remote Access Client
System Connection View Help
10.70.33.53
10.70.33.77
Remote Access Server : 10.70.33.53 Server : 10.70.33.77 Status : Authorized

Figure 3-43 New connection after the check

- If the authentication of connection request fails, a new server icon is displayed on the RAC interface. The icon color is gray, and the connection status at the bottom of the interface displays “Waiting for authentication” as shown in Figure 3-44.

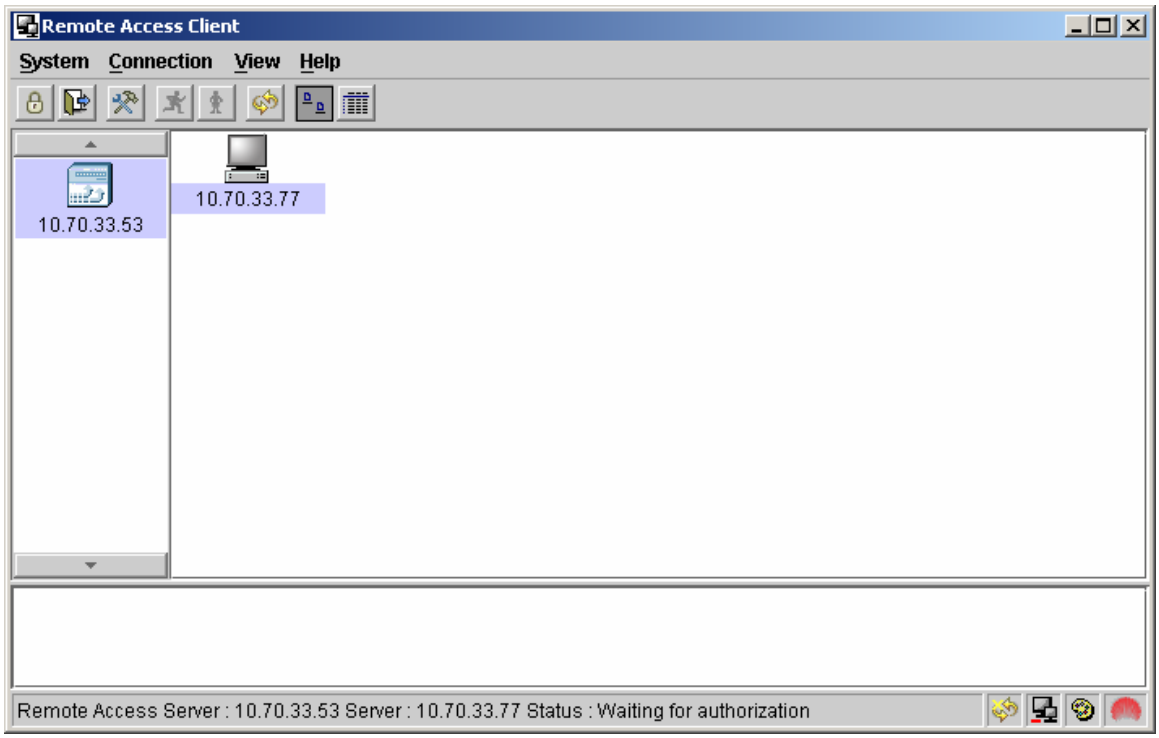

Remote Access Client
System Connection View Help
10.70.33.53
10.70.33.77
Remote Access Server : 10.70.33.53 Server : 10.70.33.77 Status : Waiting for authorization

Figure 3-44 Connection request of waiting for authorization

- If a parameter (such as the RAS address) is set wrongly on establishing a connection request, a prompt is displayed, as shown in Figure 3-45.

Figure 3-45 Prompt information of a connection request error

II. Deleting a Connection to RAS

In the RAC service interface shown in Figure 3-43, right click an “server” icon in the right window and select [Delete] in the shortcut menu, or select [Connection/Delete] in the main menu to delete the icon.

Note:

If all the “server” icons of an RAS are deleted, the RAS icon is deleted accordingly.

3.6.5 Activating/Deactivating a Connection to RAS

I. Activating a Connection to RAS

A new established connection is in the inactivated state and can be used after the activation. In the RAC service interface shown in Figure 3-43, right click an “server” icon in the right window and select [Activate] in the shortcut menu, or select [Connection/Activate] in the main menu, or click on the tool bar to activate the connection. In this case, the output window in the lower part displays the operation result and the connection status on the status bar displays “Connected”, as shown in Figure 3-46.

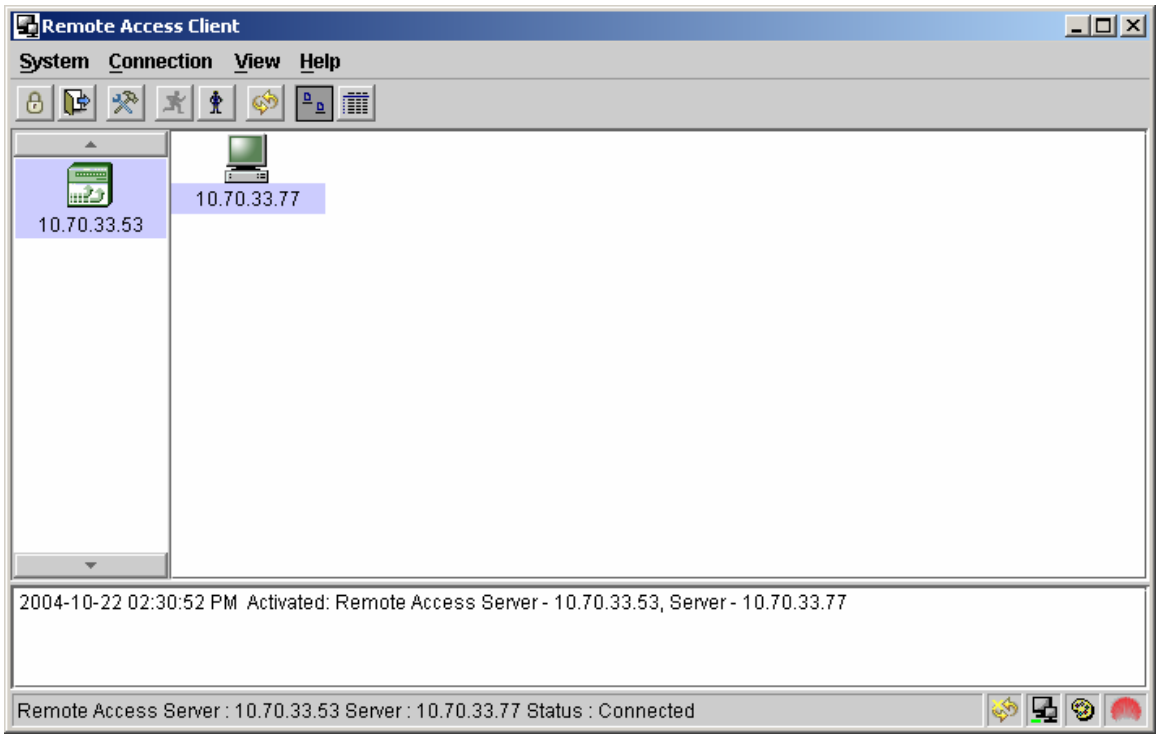

Remote Access Client
System Connection View Help
10.70.33.53
10.70.33.77
2004-10-22 02:30:52 PM Activated: Remote Access Server - 10.70.33.53, Server - 10.70.33.77
Remote Access Server : 10.70.33.53 Server : 10.70.33.77 Status : Connected

Figure 3-46 Activate a Connection to RAS

II. Deactivating a Connection to RAS

In the RAC service interface shown in Figure 3-43, right click an “server” icon. If the connection has been activated, the [Deactivate] in the shortcut menu is available. Click [Deactivate], or select [Connection/Deactivate] in the main menu, or click on the tool bar to deactivate the connection. In this case, the output window in the lower part displays operation results and the connection status on the status bar displays “Authorized”, as shown in Figure 3-47.

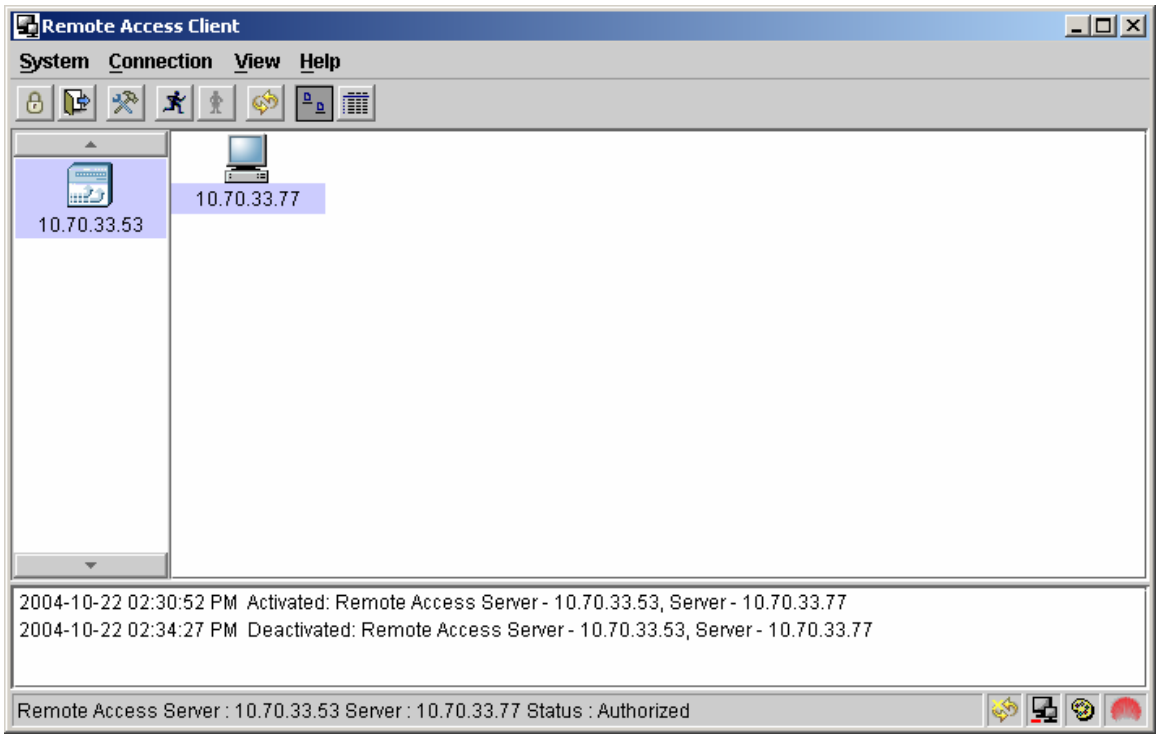

Remote Access Client
System Connection View Help
10.70.33.53
10.70.33.77
2004-10-22 02:30:52 PM Activated: Remote Access Server - 10.70.33.53, Server - 10.70.33.77
2004-10-22 02:34:27 PM Deactivated: Remote Access Server - 10.70.33.53, Server - 10.70.33.77
Remote Access Server : 10.70.33.53 Server : 10.70.33.77 Status : Authorized

Figure 3-47 Deactivating a Connection to RAS

3.6.6 Manual-Refresh/Auto-Refresh Connection Status

To ensure normal remote maintenance, you must understand the connection status change between the RAC and the RAS, and refresh related connection status in the RAC service interface timely. There are two ways to refresh a status: manual-refresh and auto-refresh.

I. Manual-Refresh

Select [Connection/Refresh], or right click an “server” icon and select [Refresh] in the shortcut menu, or click the icon on the tool bar. After the operations, the connection status is refreshed in real time. You can click the “server” icon to check the connection status change on the status bar.

II. Auto-Refresh

Select [Connection/Auto Refresh] or click the icon in the right corner. The window “Configure Auto Refresh” is displayed, as shown in Figure 3-48. Select a time interval in the “Refresh Interval”. It is recommended to adopt the default value (600 seconds).

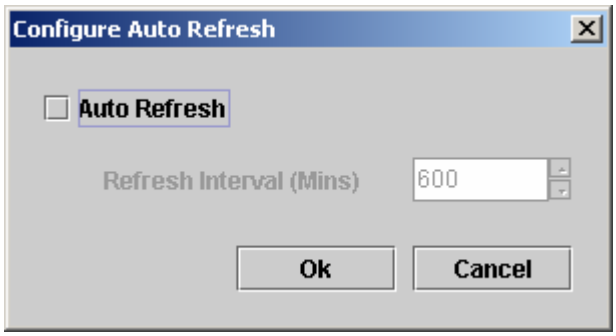


Figure 3-48 "Configure Auto Refresh" window

3.6.7 Changing RAC Interface Display Mode

There are two display modes in the RAC interface: icon display and detail display. The icon display mode is shown in Figure 3-43. Select [View/Details] in the icon mode, and then the display mode turns to detail display, as shown in Figure 3-49.

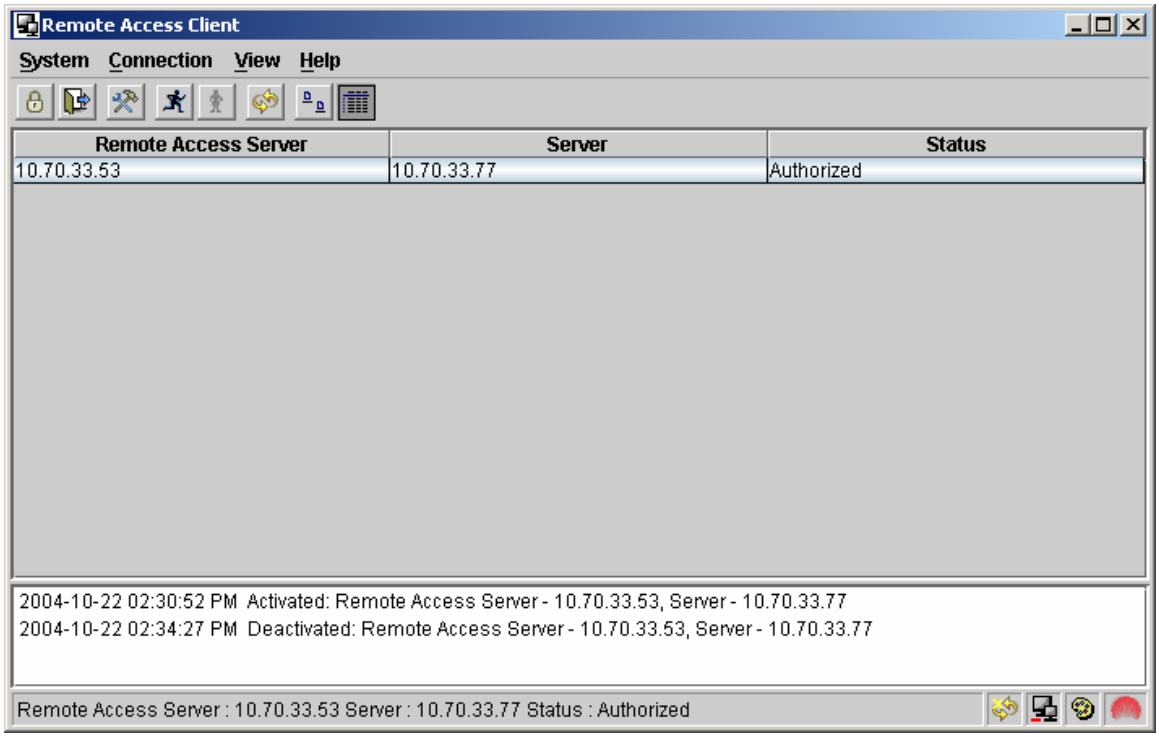

Remote Access Client
System Connection View Help
Remote Access Server
Server
Status
10.70.33.53
10.70.33.77
Authorized
2004-10-22 02:30:52 PM Activated: Remote Access Server - 10.70.33.53, Server - 10.70.33.77
2004-10-22 02:34:27 PM Deactivated: Remote Access Server - 10.70.33.53, Server - 10.70.33.77
Remote Access Server : 10.70.33.53 Server : 10.70.33.77 Status : Authorized

Figure 3-49 Detail mode

Select [View/Details] in the detail mode, and then the display mode returns to icon display.

Note:

Also, you can click or on the tool bar to change display modes.

3.6.8 Showing Online Help

Select [Help/Help] in the RAC service interface or press F1 to open the RAC online help files, as shown in Figure 3-50.

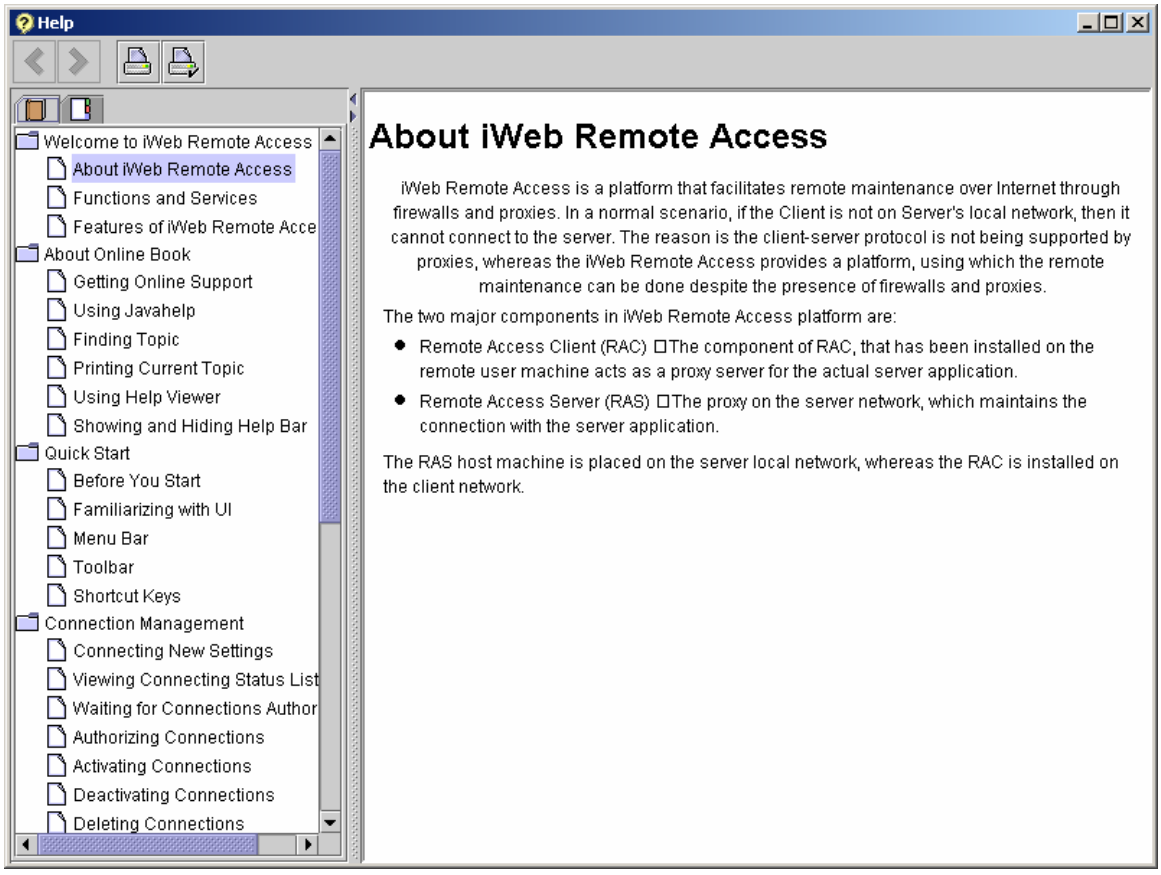

Help
Welcome to iWeb Remote Access
About iWeb Remote Access
Functions and Services
Features of iWeb Remote Acce
About Online Book
Getting Online Support
Using Javahelp
Finding Topic
Printing Current Topic
Using Help Viewer
Showing and Hiding Help Bar
Quick Start
Before You Start
Familiarizing with UI
Menu Bar
Toolbar
Shortcut Keys
Connection Management
Connecting New Settings
Viewing Connecting Status List
Waiting for Connections Author
Authorizing Connections
Activating Connections
Deactivating Connections
Deleting Connections
About iWeb Remote Access
iWeb Remote Access is a platform that facilitates remote maintenance over Internet through firewalls and proxies. In a normal scenario, if the Client is not on Server's local network, then it cannot connect to the server. The reason is the client-server protocol is not being supported by proxies, whereas the iWeb Remote Access provides a platform, using which the remote maintenance can be done despite the presence of firewalls and proxies.
The two major components in iWeb Remote Access platform are:
Remote Access Client (RAC) ☐The component of RAC, that has been installed on the remote user machine acts as a proxy server for the actual server application.
Remote Access Server (RAS) ☐The proxy on the server network, which maintains the connection with the server application.
The RAS host machine is placed on the server local network, whereas the RAC is installed on the client network.

Figure 3-50 RAC online help

3.6.9 Showing the iWeb System Version Information

In the RAC service interface, Select [Help/About], or double click the icon in the right corner. The window “About Remote Access Client” is displayed to display the version information of the iWeb remote maintenance access system, as shown in Figure 3-51.

Figure 3-51 "About Remote Access Client" window

3.6.10 Logging Out RAC

In the RAC service interface, select [System/Logout]. A confirmation window is displayed, as shown in Figure 3-52.

Figure 3-52 Logout confirmation window

Click <Yes> to return to the RAC login interface shown in Figure 2-21.

3.6.11 Exiting RAC Service Interface

In the RAC service interface, select [System/Exit], or click the icon on the tool bar to close the RAC service interface.

Note:

In the RAC service interface, if you click the button on the top right corner, you can just hide the interface, but not exit the RAC service interface. If there is still a "client proxy" icon on the status bar, click the icon to open the RAC service interface.

3.7 A Typical Maintenance Example

3.7.1 Description of Example

The following takes a specific configuration application example to describe how to configure the RAC and the RAS.

A server with the IP address of 10.10.10.1 needs remote maintenance; the server type is SoftX3000; The IP address of an RAS which is in the same subnet with the server is 10.10.10.9. The RAS accesses Internet directly.

A maintenance terminal used by a remote maintenance engineer accesses the Internet through an RAC and a proxy server to maintain remotely. The IP address of the maintenance terminal is 10.10.30.1; the IP address of the RAC is 10.10.30.2; the IP address of the proxy server is 10.10.30.9; the port number of the proxy server is 80.

The following describes remote maintenance steps:

3.7.2 Configuring RAS Data

Proceed as follows:

1) For details, refer to “3.2.1 Configuring IP Address and Ports”, ”3.2.2 Configuring Multi-Language Attribute”, and ”3.2.3 Configuring Log Functions”. The IP address is set to 10.10.10.9. Other parameters are set to default values.
2) Start RAS service and refer to “3.2.5 Configuring Server Types” to add SoftX3000” in server types..
3) Refer to “3.2.6 Configuring Server Instances” to add a server instance whose IP address is 10.10.10.1 and type is SoftX3000.
4) Refer to “3.2.4 Configuring Connection Instances” to add a connection from RAC (IP: 10.10.30.2) to a server (IP: 10.10.10.1) in “Client Session List”.

3.7.3 Configuring the RAC Data

Proceed as follows:

1) For details, refer to “3.3.1 Configuring System Attribute File” and “3.3.2 Configuring Log Functions”. “Language” is set to “en”; “Country” is set to “US”; other options are set to default values.
2) Start the RAC service, and refer to “3.3.3 Configuring Proxy Information” to set the IP address of the proxy server as 10.10.30.9 and the port number of the proxy server as 80.
3) Refer to “3.3.4 Configuring Maintenance Terminal Access Strategy” to add the maintenance terminal (IP: 10.10.30.1) to the IP address ranges of clients that can access the RAC.

3.7.4 Creating Connection from RAC to RAS

Proceed as follows:

1) Refer to “3.5.4 Adding/Removing a Connection to RAS” to add a connection from RAC to RAS. Connection parameters are set to default values.
2) Because the connection has been configured on RAS, the system automatically checks and authenticates the connection request. If the connection instance has not been configured on the RAS, refer to “3.4.3 Review Connection Request Manually” to check the request manually.
3) After successful authentication, the connection between RAC and RAS is established and the access strategy (maintainable server types and instances) configured on the RAS is synchronized to the RAC.

3.7.5 Starting Remote Maintenance

Proceed as follows:

1) Start remote maintenance program on a maintenance terminal to connect the RAC. The connection mode depends on the remote maintenance program. For example, use the Telnet mode to connect the RAC.
2) The RAC authenticates a maintenance terminal access authority based on maintenance terminal access control configuration and authenticates the connection request based on access strategy. After the authentication is passed, you can receive and transmit maintenance data.
3) During the maintenance, the connection between RAC and RAS can be regarded as a data channel between a maintenance terminal and a server to be maintained.

3.7.6 Ending Remote Maintenance

Deactivate/delete the corresponding connection or instance (including connection instance and server instance) on the RAC or the RAS to end remote maintenance.

For details, refer to the following sections:

- Configuring Connection Instances
- Establishing/ Deleting a Connection to RAS
- Activating/Deactivating a Connection to RAS

3.8 FAQ on Remote Maintenance

3.8.1 One RAC Cannot Activate Multiple Maintenance Terminals?

This is stipulated by the system. One RAC can only activate one maintenance terminal at a time. In other words, only one maintenance terminal can be maintained remotely.

3.8.2 RAC Cannot Refresh Connection Status or Start Connection?

The following describes possible reasons and corresponding handling methods.

- Proxy information such as the IP address or port configuration of a proxy server is incorrectly set on the RAC.
- The RAS background service is not started. Refer to “3.4.1 Starting RAS Background Service”.
- The connection between RAC or a proxy server and RAS is disconnected. If you fail to retry the connection, check and restore the network connection between RAC or a proxy server and RAS.

3.8.3 Maintenance Terminal Cannot Receive Response from Server in Time?

If the port is a bi-directional port, reporting port or time out bi-directional port, try to change its performance attribute. You can adopt the maximum performance or change the port attribute into blocking bi-directional port so that a maintenance terminal can receive the response from a server timely.

Appendix A Description of RAS Installation Directory

The default installation directory of RAS is C:\Remote Access\Server. Table A-1 describes its programs and files.

Table A-1 List of RAS Installation Directory

Subdirectory	Important file name	Function
NA	log.txt	Log file, which records routine maintenance information and connection status.
	run.bat	Batch file, which starts the RAS background service.
_uninst	NA	It contains the uninstallation program of RAS software.
bin	NA	It contains the command execution files of Tomcat.
classes	NA	It contains class files of Java environment.
common	NA	It contains archive files of Tomcat together with the lib directory and the server directory.
conf	LogConfig.xml	RAS configuration file, which configures log functions of RAS.
	server.xml	RAS configuration file, which binds the IP address of RAS, and to configure HTTP and HTTPS ports.
lib	NA	It contains archive files of Tomcat together with the common directory and the server directory.
logs	NA	Web server directory
server	NA	It contains archive files of Tomcat together with the common directory and the server directory.
webapps	NA	It stores the web applications, which should comply with standard web directory of J2EE stipulation.
work	NA	It stores temporary files.

Appendix B Description of RAC Installation Directory

The default installation directory of RAC is C:\Remote Access\Client. The following describes its programs and files.

Table B-1 List of RAC Installation Directory

Subdirectory	Important file name	Function
Root directory	RemoteAccessClient.exe	Executable file, which starts RAC.
	run.bat	Batch file, which sets JAVA work environment and some system parameters.
	log.txt	Log file, which records routine maintenance information and connection status.
_uninst	NA	It contains the uninstallation program of RAC software.
classes	NA	It contains class files of JAVA environment.
conf	LogConfig.xml	RAC configuration file, which configures log functions of RAC.
	system.properties	RAC configuration file, which configures such parameters as RAC language, country, display model, and maximum number of connected clients.
dist	NA	It stores the installation program.
help	NA	Help file directory
icon	NA	System icon directory, which is to store icons used by the system.
lib	NA	It is to store grandfather files of Tomcat.
logs	NA	Web server directory

HUAWEI

U-SYS SoftX3000 SoftSwitch System
BAM User Manual

Part 3 Appendix

Table of Contents

Appendix A Glossary A-1

Appendix B Acronyms and Abbreviations B-1

Appendix A Glossary

Term	Definition
BAM	As the element management system (EMS) layer of telecommunication management network, BAM provides fault, security, accounting, performance, and security (FCAPS) functions. It provides the MML command to configure and maintain the equipment; it also supports the client-server architecture and can connect to multiple clients.
Firewall	Firewall is one or more systems that forcedly carry out the access control strategy between two networks. There are two types of firewalls: one that enables certain types of services, and one that disables services.
HTTP	It transmits hyper text files over Internet. One end needs HTTP client program; the other end needs HTTP server program. HTTP is an important protocol used in the world wide web.
Proxy server	Proxy server is located between clients (such as Web browser) and application servers. It transfers or intercepts service requests which are sent from servers to application servers. It also transfers or intercepts service data from application servers to servers. Also, it provides some service functions.
RAC	RAC is a part of the iWeb remote maintenance access system. It reviews maintenance requests from clients, collects, and transfers maintenance data. In the iWeb system, clients can access remote equipment servers only through RAC and RAS.
RAC administrator	An RAC administrator maintains configuration data of RAC, starts and closes RAC, and establishes and maintains the connection between RAC and RAS.
Remote maintenance	It means some maintenances are executed remotely. “Maintenance” can be defined as a process of sending a command to manage equipment attributes in the telecom network. Because operator is far away from equipments to be maintained, the operation is called “remote maintenance”.
RAS	RAS is a part of the iWeb remote maintenance access system. It reviews connection requests from RAC, configures equipment servers to be maintained, and collects and transfers maintenance responses. In the iWeb system, client can access remote equipment servers only through RAC and RAS.
RAS administrator	RAC administrator maintains configuration data of RAS, starts and closes RAS, reviews connection requests from RAC, and collects and transfers maintenance responses.

Appendix B Acronyms and Abbreviations

Abbreviation	Full name
B	
BAM	Back Administration Module
C	
CPU	Center Processing Unit
D	
DLL	Dynamic Link Library
DHCP	Dynamic Host Configuration Protocol
H	
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol Secure
I	
IP	Internet Protocol
N	
NetBIOS	Network Basic Input/Output System
R	
RAC	Remote Access Client
RAM	Random Access Memory
RAS	Remote Access Server
S	
SQL	Structured Query Language
T	
TCP	Transmission Control Protocol
W	
WWW	World Wide Web

Index

B

background of iWeb system, *2-1*
basic operations
  check and process the alarm, *1-22*
  check log file, *1-24*
  checking the system integrity, *1-21*
  generating verification files, *1-18*
  starting SysPatron, *1-19*
  stopping SysPatron, *1-20*

C

comparason between ordinary anti-virus software and syspatron
  comparison results, *1-1*
  Features of Ordinary Anti-Virus Software, *1-1*
  Features of SysPatron, *1-1*
connection instances, *2-45*
  add, *2-46*
  canceling authentication, *2-51*
  delete, *2-50*
  refresh, *2-51*
connection status, *2-82*
  auto-refresh, *2-82*
  manual-refresh, *2-82*
connection to RAS, *2-75*
  activating, *2-81*
  deactivating, *2-81*
  delete, *2-80*
  establishing, *2-75*

F

FAQs, *1-25*
function description, *1-2*
  alarm management, *1-6*
  integrity detection, *1-5*
  log management, *1-5*
  progress monitoring, *1-4*
  system verification, *1-3*

G

generation of verification files, *1-3*
  automatic generation during the installation of the SysPatron, *1-3*
  generation by tool after the installation of the SysPatron, *1-3*

H

hardware configuration, *1-6*
  CPU, *1-6*
  hard disk, *1-6*
  network card, *1-6*
  RAM, *1-6*

I

installation check
  check for the installation directory, *1-13*
  check whether the menu item of the SysPatron exists, *1-13*
  check whether the SysPatron is started normally, *1-14*
  check whether the system monitoring functions normally, *1-14*
  check whether the timing detection function can be used normally, *1-15*
  check whether verification files for programs and files in the file list are generated, *1-14*
installation of iWeb system, *2-16*
integrity detection
  manual detection, *1-5*
  timing detection, *1-5*

J

JDK software, *2-18*
  installing, *2-18*

setting enviroment variables, *2-20*

O

Operating principle of iWeb system, *2-6*
operation on verification files, *1-18*
add a file to the list, *1-19*
clearing up list, *1-19*
deleting a file from the list, *1-19*
generating verification files, *1-19*

P

progress monitoring
handling measurement after real-time verification, *1-4*
specific steps of real-time verification, *1-4*

R

RAC operation, *2-60*
basic operation, *2-74*
data configuration, *2-60*
interface, *2-39*
RAC software, *2-31*
installation, *2-31*
installation check, *2-31*
RAS operation, *2-40*
basic operation, *2-66*
data configuration, *2-40*
interface, *2-37*
RAS software, *2-23*
installation, *2-23*
installation check, *2-29*

S

safety problem of BAM, *1-1*
illegal attack, *1-1*
third-party software, *1-1*
server instances, *2-56*
add, *2-56*
delete, *2-59*
refresh, *2-60*
server types, *2-52*
add, *2-52*
delete, *2-56*
service models of iWeb system, *2-8*
remote access client, *2-9*
remote access server, *2-8*
software and hardware configuration, *2-14*
software configuration, *1-7*
matched software, *1-7*
software composition of the SysPatron, *1-7*
software installation, *1-9*
closing all application programs, *1-10*
installation check, *1-13*
installing the operating system and the server application software, *1-9*
killing viruses completely by latest anti-virus software, *1-10*
software uninstalling, *2-32*
system functions of iWeb system, *2-11*
access control, *2-11*
connection management, *2-11*
data compression and encryption, *2-12*
traversing firewalls and proxy servers, *2-12*
two-way data transmission, *2-12*

T

technical features of iWeb system, *2-12*
typical configurations of iWeb system, *2-1*

U

uninstalling software, *1-15*